# ANALISIS KEAMANAN JARINGAN WIRELESS LAN (WLAN) PADA PT. PLN (PERSERO) WILAYAH P2B AREA SORONG

**Sonny Rumalutur**
Jurusan Teknik Elektro
Politeknik Katolik Saint Paul Sorong
Email:sonny.rmltr@gmail.com

**ABSTRAK**

Penelitian ini membahas tentang analisis keamanan Wireless Local Area Network (Wireless LAN) di PT. PLN (Persero) Wilayah P2B Area Sorong terhadap serangan luar pada protokol Wireless Protected Access (WPA), Web Proxy, dan Virtual Private Network (VPN), digunakan untuk menyerang LAN.
Tiga jenis perangkat lunak yang digunakan sebagai penyerang yaitu, penyerang Network Stumbler, Aircrack dan Wireshark. Perangkat lunak tersebut digunakan di laptop pada jarak 5m sampai 25m dari titik akses LAN Nirkabel.
Dari hasil experimen terlihat waktu tercepat direspon oleh Protokol WPA diberikan oleh penyerang Network Stumbler, diikuti oleh Aircrack dan Wireshark.

Kata Kunci : *Wireless Protected Access, Web Proxy* dan *Virtual Private Network.*

## Pendahuluan

Perkembangan teknologi komunikasi ini juga didukung dengan semakin meningkatnya kemajuan infrastruktur dan teknologi. Salah satu perkembangan teknologi komunikasi dan informasi ini adalah komunikasi menggunakan wireless.
Ini ditandai dengan perkembangan munculnya peralatan nirkabel yang telah menggunakan standar protokol Wireless Fidelity (WiFi) yang berbasiskan standar IEEE 802.11.

Penggunaan jaringan yang semakin luas di dunia bisnis dan pertumbuhan kebutuhan penggunaan internet online services yang semakin cepat mendorong untuk memperoleh keuntungan dari shared data dan shared resources. Dengan Wireless Local Area Network (Wireless LAN) pengguna dapat mengakses informasi tanpa mencari tempat untuk plug in dan dapat menset up jaringan tanpa menarik kabel. Wireless LAN dapat mengatasi masalah kekurangan wired network, karena mempunyai kelebihan dibandingkan antara lain sebagai berikut: *Mobility*, *Scalability*, *Installation Speed and Simplicity*, *Installation Fleksibility*, *Reduced cost of ownership.*

Teknologi informasi bukan Teknologi wireless yang menghasilkan berbagai kemudahan juga membawa dampak bagi para pengguna jasa internet baik industri, pendidikan dan user mandiri. Perkembangan ini juga dapat dirasakan secara langsung oleh kita dengan banyaknya wireless hotspot yang tersedia dimana-mana.

Selain dapat membantu serta melahirkan berbagai inovasi yang positif. Tetapi juga melahirkan sisi negative. Dan ini selalu terjadi tidak terkecuali pada perkembangan wireless.

Untuk membatasi permasalahan yang meluas, maka permalahan yang akan dibahas dalam penelitian ini dibatasi pada infrastruktur protokol keamanan Wireless LAN. Analisis dilakukan

melalui beberapa kajian white paper dan wacana yang ada serta melakukan eksperimen dengan melakukan serangan (attack) terhadap infrastruktur Wireless LAN. Protokol keamanan Wireless LAN yang digunakan dalam penelitian yaitu Wireless Protected Access (WPA), Web Proxy dan Virtual Private Network (VPN). Dengan menggunakan 3 *tools attacker* yaitu Network Stumbler, Aircrack dan Wireshark

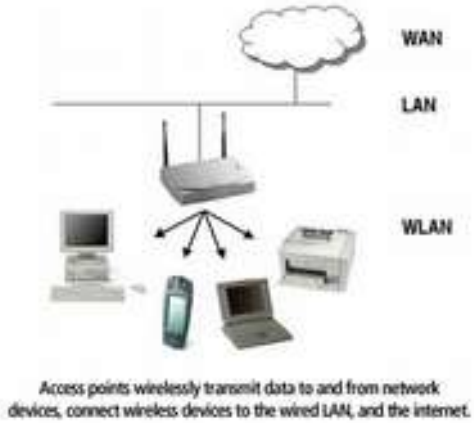
Adapun tujuan penulisan tesis ini adalah sebagai berikut :

Menguji sejauh mana kemampuan keamanan protocol WPA, Web Proxy dan Virtual Private Network (VPN), terhadap serangan dari Software Network Stumbler, Aircrack dan Wireshark.

**Tinjauan Pustaka**

Wireless LAN (WLAN) atau Wireless Fidelity (Wi-Fi), yaitu teknologi yang digunakan untuk mentransmisikan data yang berjalan pada jaringan komputer lokal tanpa penggunaan kabel dengan menggunakan infrastruktur dan media transmisi yang baru, dalam hal ini adalah gelombang radio. Agar berbagai macam produk Wireless LAN yang berasal dari vendor yang berlainan dapat saling bekerja sama/kompatibel pada jaringan, maka dibuatlah suatu standar untuk teknologi ini, yang disebut dengan IEEE (Institute for Electrical and Electronic Engineers) 802.11.

Wireless Local Area Network sebenarnya hampir sama dengan jaringan LAN, akan tetapi setiap node pada WLAN menggunakan wireless device untuk berhubungan dengan jaringan node pada WLAN menggunakan channel frekuensi yang sama dan SSID yang menunjukkan identitas dari wireless device. Tidak seperti jaringan kabel, jaringan wireless memiliki dua mode yang dapat digunakan: infastruktur dan Ad-Hoc. Konfigurasi infrastruktur adalah komunikasi antar masing-masing PC melalui sebuah access point pada WLAN atau LAN. Komunikasi Ad-Hoc adalah komunikasi secara langsung antara masing-masing komputer dengan menggunakan piranti wireless. Penggunaan kedua mode ini tergantung dari kebutuhan untuk berbagi data atau kebutuhan yang lain dengan jaringan berkabel.




Gambar 1. Konfigurasi WLAN

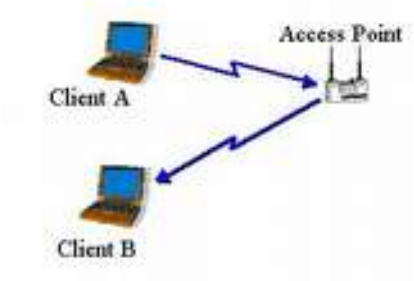
Jaringan *Wireless LAN* terdiri dari komponen *wireless user* dan *access point* dimana setiap *wireless user* terhubung ke sebuah *access point*.

Topologi *Wireless LAN* dapat dibuat sederhana atau rumit dan terdapat dua macam topologi yang biasa digunakan, yaitu sebagai berikut [3] :

**Sistem Infrastructure**

Wireless lan memiliki SSID (Service Set Identifier) sebagai nama jaringan wireless tersebut. Sistem penamaan SSID dapat diberikan maksimal sebesar 32 karakter. Karakter-karakter tersebut juga dibuat case sensitive sehingga SSID dapat lebih banyak variasinya.

Dengan adanya SSID maka wireless lan itu dapat dikenali. Pada saat beberapa komputer terhubung dengan SSID yang sama, maka terbentuklah sebuah jaringan infrastruktur.




Gambar 2. Jaringan infrastruktur [3]

**Sistem Adhoc**

Ad-hoc mode digambarkan sebagai jaringan peer-to-peer atau juga di sebut dengan Independent Basic Service Set (IBSS).yang digunakan bila sesama pengguna dengan saling mengenal *Service Set Identifier* (SSID), dimana jaringannya terdiri dari beberapa komputer yang masing-masing dilengkapi dengan *Wireless Network Interface Card* (*Wireless NIC*).


Gambar 2. Jaringan AdHoc [3]

**Keamanan *Wireless LAN***

Jaringan wireless memiliki lebih banyak kelemahan dibanding dengan jaringan kabel (wired). Kelemahan jaringan wireless secara umum dapat dibagi menjadi 2 jenis, yakni kelemahan pada konfigurasi dan kelemahan pada jenis enkripsi yang digunakan. Salah satu contoh penyebab kelemahan pada konfigurasi karena saat ini untuk membangun sebuah jaringan wireless cukup mudah [7]. Banyak vendor yang menyediakan fasilitas yang memudahkan pengguna atau admin jaringan sehingga sering ditemukan wireless yang masih menggunakan konfigurasi wireless default bawaan vendor.

Secara umum, terdapat 3 (tiga) kata kunci dalam konsep keamanan jaringan:

Tabel 1. Konsep Keamanan Jaringan [6]

| Konsep | | Keterangan |
|---|---|---|
| 1. | Resiko atau tingkat bahaya : | Resiko berarti berapa kemungkinan keberhasilan para penyusup dalam mengakses ke dalam jaringan komputer lokal yang dimiliki melalui konektivitas jaringan lokal ke Wide Area Network (WAN) antara lain sebagai berikut: |
| | - Denial of Service : | Menutup penggunaan utilitas jaringan normal dengan cara menghabiskan jatah Central Processing Unit (CPU), memory maupun |

| | | |
|---|---|---|
| | | bandwidth. |
| | - Write Access : | Mampu melakukan proses menulis atau menghancurkan data dalam sistem. |
| 2. | Ancaman : | Orang yang berusaha memperoleh akses secara ilegal ke dalam jaringan. |
| 3. | Kerapuhan Sistem : | Seberapa jauh perlindungan yang bisa diterapkan kepada network dari seseorang dari luar sistem yang berusaha memperoleh akses ilegal terhadap jaringan dan kemungkinan orang dari dalam sistem memberikan akses kepada dunia luar yang bersifat merusak sistem jaringan tersebut. |

Keamanan Wireless LAN, terdapat beberapa faktor yang menentukan sejauh mana keamanan ingin didapatkan yaitu penyerang (attacker), ancaman (threats), potensi kelemahan (potential vulnerabilities), aset yang beresiko (asset at risk), perlindungan yang ada (existing safeguard) dan perlindungan tambahan (additional control).

Mekanisme keamanan dalam *Wireless LAN* adalah hal penting dalam menjaga kerahasiaan data. Proses enkripsi di dalam mekanisme keamanan merupakan proses pengkodean pesan untuk menyembunyikan isi. Algoritma enkripsi modern menggunakan kunci kriptografi dimana hasil enkripsi tidak dapat didekripsi tanpa kunci yang sesuai.

Tabel 2. Layanan perlindungan keamanan [1]

| Kategori | | Penjelasan |
|---|---|---|
| 1. | **Kerahasiaan *(Confidentiality)*** | yaitu mencegah pihak yang tidak berhak mengakses membaca informasi yang bersifat rahasia dan harus aman dari pengkopian. |
| 2. | **Integritas *(Integrity)*** | yaitu menjamin data yang diterima tidak mengalami perubahan selama dikirimkan, baik itu dimodifikasi, diduplikasi, dikopi atau dikembalikan. |
| 3. | **Otentikasi *(Authentication)*** | yaitu suatu layanan keamanan yang diberikan untuk meyakinkan bahwa identitas pengguna yang melakukan komunikasi di jaringan yang benar. |
| 4. | **Tidak terjadi penyangkalan *(Non-repudiation)*** | yaitu mencegah baik penerima maupun pengirim menyangkal pesan yang dikirim atau diterimanya. |
| 5. | **Ketersediaan *(Availability)*** | yaitu menjamin ketersediaan suatu sistem untuk dapat selalu digunakan setiap ada permintaan dari pengguna. |
| 6. | **Akses Kendali *(Access Control)*** | yaitu membatasi dan mengontrol akses setiap pengguna. |

**Serangan *Wireless LAN***

Jaringan wireless sangatlah rentan terhadap serangan, hal ini dikarenakan jaringan wireless tidak dapat dibatasi oleh sebuah gedung seperti yang diterapkan pada jaringan berbasis kabel. Sinyal radio yang dipancarkan oleh perangkat wireless dalam melakukan proses transmisi data didalam sebuah jaringan dapat dengan mudah diterima/ditangkap oleh pengguna komputer lain selain pengguna dalam satu jaringan hanya dengan menggunakan perangkat yang kompatibel dengan jaringan wireless seperti kartu jaringan wireless.

**Protokol *Wireless Protected Access***

*Wireless Protected Access* (WPA) ditawarkan sebagai solusi keamanan yang lebih baik daripada WEP. WPA merupakan bagian dari standar yang dikembangkan oleh *Robust Security Network* (RSN). WPA dirancang untuk dapat berjalan dengan beberapa sistem perangkat keras yang ada saat ini, namun dibutuhkan dukungan peningkatan kemampuan perangkat lunak (*software upgrade*).

Pada perkembangan selanjutnya, dimana algoritma RC4 digantikan oleh algoritma enkripsi baru yaitu *Advance Encryption System* (AES) dengan panjang kunci sepanjang 256 bit. Dukungan peningkatan keamanan *Wireless LAN* yang disediakan WPA adalah meliputi Otentikasi dan Kendali Akses, Enkripsi dan Integritas Data. Standar tersebut ternyata masih mempunyai banyak titik kelemahan dalam keamanan. Karena itulah dikembangkan pembagian lapisan keamanan yang sudah ada menjadi 3 (tiga) yaitu:

1. Lapisan *Wireless LAN, a*dalah lapisan yang berhubungan dengan proses transmisi data termasuk juga untuk melakukan enkripsi dan deskripsi.
2. Lapisan Otentikasi, adalah lapisan dimana terjadi proses pengambilan keputusan mengenai pemberian otentikasi kepada pengguna berdasarkan informasi identitas yang diberikan. Dengan kata lain adalah untuk membuktikan apakah identitas yang diberikan sudah benar.
3. Lapisan Kendali Akses, adalah lapisan tengah yang mengatur pemberian akses kepada pengguna berdasarkan informasi dari lapisan otentikasi.

**Otentikasi dan Kendali Akses dalam WPA**

Otentikasi yang didukung oleh WPA adalah otentikasi dengan menggunakan *preshared key* dan otentikasi dengan menggunakan *server based key*. Otentikasi dengan *preshared key* adalah model otentikasi dengan menggunakan WEP [2]. Sedangkan otentifikasi dengan *server based key* adalah model otentifikasi dengan menggunakan akses kontrol.

WPA mendefinisikan dua macam kunci rahasia, yaitu *pairwise key* dan *group key*. *Pairwiseway* adalah kunci yang digunakan antara *wireless user* dengan *access point*, Kunci ini hanya dapat digunakan dalam transmisi data di antara kedua belah pihak tersebut (*unicast*).
*Pairwise key* maupun *group key* mempunyai manajemen kunci tersendiri yang disebut dengan *pairwise key hierarchy* dan *group key hierarchy*

**Enkripsi dalam WPA**

WPA menggunakan protokol enkripsi yang disebut dengan *Temporary Key Integrity Protocol* (TKIP). TKIP mendukung pengubahan kunci (*rekeying*) untuk *pairwise key* dan *group key*.
Fitur-fitur keamanan yang disediakan oleh TKIP adalah:

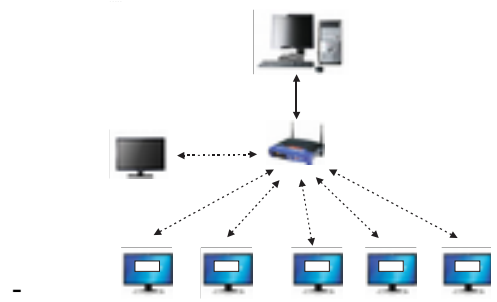
1. Penambahan besar ukuran *initialization vector* untuk mencegah terjadinya pengulangan nilai *initialization vector*.
2. Pengubahan cara pemilihan *initialization vector* untuk mencegah terjadinya *weak key*, juga mencegah terjadinya kemungkinan *replay attack*.
3. Pengubahan kunci enkripsi untuk setiap paket yang dikirimkan (*per packet key mixing*).
4. Penggunaan *message integrity protocol* yang lebih baik untuk mencegah terjadinya modifikasi pesan.

5. Penggunaan mekanisme untuk melakukan distribusi maupun perubahan terhadap kunci rahasia yang digunakan.

## METODE PENELITIAN

Penelitian difokuskan kepada bagaimana menformulasikan permasalahan yang ada dan diidentifikasi dan dirumuskan berdasarkan aspek keamanan protokol Wireless LAN. Kemudian menyusun suatu hipotesa sebagai jawaban atau kesimpulan awal dan strategi untuk menguji apakah hipotesa tersebut merupakan jawaban atas permasalahan yang ada.

Dalam penelitian ini penulis menggunakan beberapa tahapan yang diawali dengan :
Membuat suatu perancangan dengan menggunakan topologi infrastruktural dengan 5 (lima) wireless user yang dihubungkan dengan 1 (satu) *server* melalui 1 (satu) *access point* dan 1 (satu) penyerang.



**Gambar 3. Percobaan Serangan**

Melakukan percobaan serangan terhadap infrastruktur *Wireless LAN* dengan menggunakan protokol keamanan WPA, *Web Proxy* dan *Virtual Private Network* dengan perbedaan jarak antara penyerang dan *access point* dengan kekuatan signal yang berbeda yaitu dengan posisi jarak 5 meter, 10 meter, 15 meter, 20 meter, 25 meter.

Gambar 4. Posisi Percobaan Penyerang

**Analisis Data**

Data dianalisis dengan menggunakan beberapa tahapan pengujian sebagai berikut:

a. Mengidentifikasikan atau memonitor konfigurasi keberadaan *hotspot* dengan menggunakan *software Network Stumbler 0.4.0.*
b. Kemudian berhubungan dengan membuka *wireless network connection.*
c. Berusaha memecahkan *password* pada *access point* yang digunakan menggunakan *software Aircrack-ng-0.9.3-win* .
*e.* Serangan tersebut diukur data yang dikirim, data yang diterima dan data yang hilang menggunakan *software Network Stumbler 0.4.0* .

Uji coba serangan pemanipulasian *IP address* dilakukan dengan 2 metoda pengujian :

- ***Metode 1*** **:**
  - Melakukan koneksi berdasarkan informasi *MAC Address* dan Mendapatkan *IP Address* lalu membuka *session* koneksi *Wireless* dengan melakukan *login ke Web Proxy* dan terhubung dengan *server.*
  - Melakukan penyadapan paket untuk mendapatkan *MAC Address* yang sah dengan menggunakan *software Network Stumbler* serta memalsukan *MAC Address* miliknya dan melakukan koneksi dengan *access point* berdasarkan *MAC address* yang dipalsukan.

- ***Metode 2*** **:**
  - Melakukan koneksi dengan *access point* berdasarkan *MAC Address* yang dipalsukan dan mendapatkan *IP Address* dan koneksi *Wireless LAN* dibuka dengan melakukan *login* ke *Web Proxy.*
  - Melakukan koneksi dengan *access point* berdasarkan *MAC address* yang dipalsukan dan mendapatkan *IP Address* dan tidak dapat membuka *session* koneksi *Wireless LAN* saat *login* ke *Web Proxy*.

**Hasil yang diharapkan pada sisi penyerang :**
Serangan berhasil jika *IP Address* dari *wireless user* dan penyerang berbeda (yang didapat dari *server*) dan Serangan gagal jika *IP Address* dari *wireless user* dan penyerang sama (yang didapat dari *server*). Jika serangan gagal maka dilakukan konfigurasi *IP Address* secara manual pada salah satu *device* supaya mendapatkan *IP Address* berbeda.

## HASIL DAN PEMBAHASAN

Dalam merancang model keamanan, aset jaringan yang beresiko perlu diperhatikan seperti titik kelemahan dalam sistem keamanannya, atau gangguan yang datang dari sipenyerang, serta motivasi serangan tersebut untuk masing-masing potensi kelemahan yang ada. Mengenai hal tersebut sangat diperlukan untuk mengambil suatu tindakan perlindungan keamanan yang dibutuhkan.

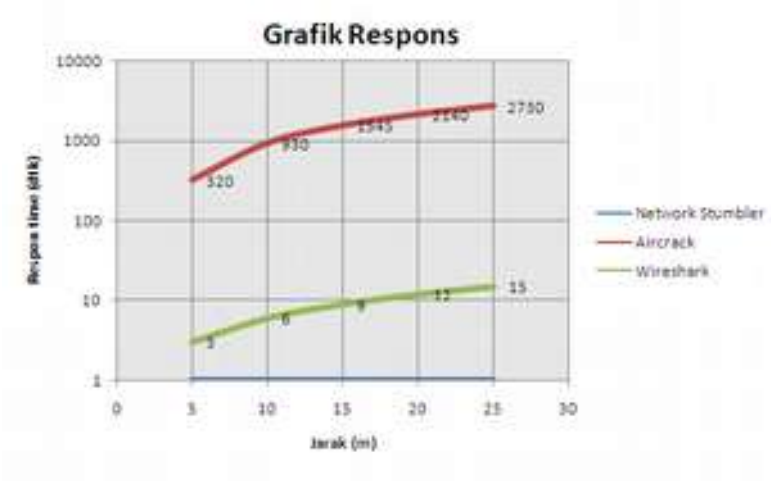
### Hasil Analisis dengan Protokol WPA

Dengan Protokol WPA dapat mengatasi kelemahan pada integritas data dan ketersediaan pada sistem. Dan penulis mencoba melakukan percobaan untuk membuktikan kelemahan protokol WPA jika diterapkan pada *Wireless LAN*, yaitu dengan melakukan serangan terhadap *encryption* (*Network Key* atau *password*) yang digunakan oleh *access point.*

**Tabel 3. Hasil Percobaan Serangan terhadap Protokol WPA**

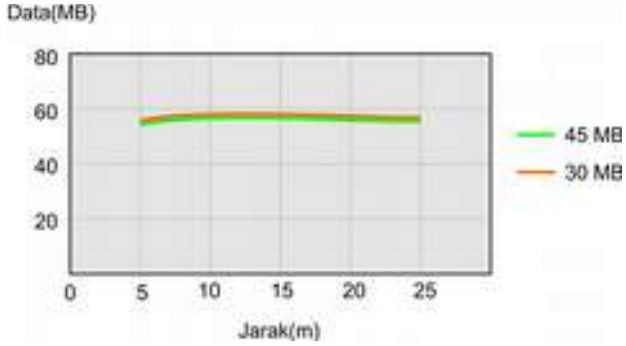
| Jarak (m) | Network Stumbler | Aircrack | Wireshark |
|---|---|---|---|

| | Respon time rata2 (detik) | Respon time rata2 (detik) | Respon time rata2 (detik) |
|---|---|---|---|
| 5 | 0 | 320 | 3 |
| 10 | 0 | 930 | 6 |
| 15 | 0 | 1545 | 9 |
| 20 | 0 | 2140 | 12 |
| 25 | 0 | 2730 | 15 |

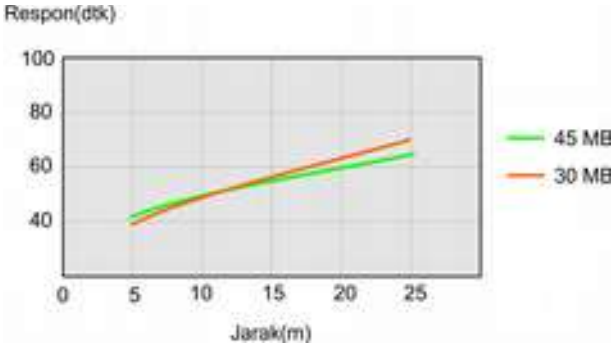



Gambar 5. Grafik Respons Time terhadap Protokol WPA.

Dari grafik Respons Time terlihat bahwa Network Stumbler yang paling cepat mendeteksi sistem keamanannya sedangkan Aircrack yang paling lambat. Kemudian juga melakukan serangan terhadap pengambilan data yang dikirimkan oleh *wireless user* dengan menggunakan protokol WPA ke *server.* Dan hasilnya bisa dengan mudah terkoneksi dengan *access point*. Dan juga dapat melakukan pengambilan data sehingga data yang diterima mengalami masalah seperti dijelaskan pada gambar 6. dan gambar 7.

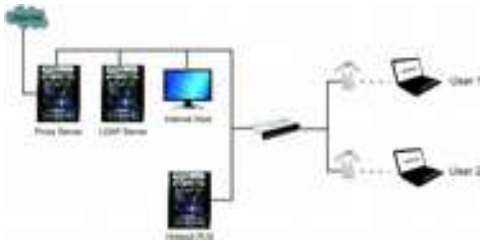



Gambar 6. Jumlah Paket Data yang Diterima.



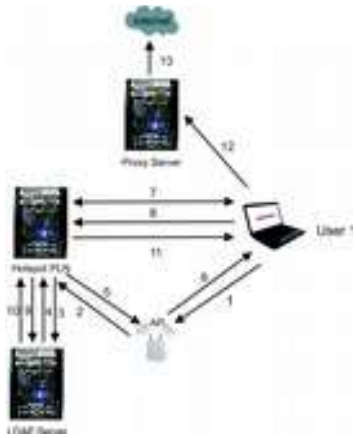

Gambar 7. Respon Time Data yang diterima di Server.

**Hasil Analisis Dengan Keamanan *Web Proxy***



Gambar 8. Arsitektur Wireless LAN

Dari gambar tersebut arsitektur *Wireless LAN* dan jaringan kabel merupakan bagian dari jaringan terintegrasi. Akses kontrol terhadap *device* yang ingin melakukan koneksi dilakukan dengan menggunakan *MAC Address* dari pengguna yang disimpan dalam *server* LDAP (*Lightweight Direction Access Protocol*). Proses otentikasi ke dalam jaringan dilakukan dengan melalui *Web Proxy* yang menggunakan protokol *Secure Socket Layer* (SSL). SSL adalah protokol keamanan yang bekerja di atas lapisan ke 4 (empat) OSI (*transport layer*), dimana semua data-data yang melalui protokol ini akan dienkripsi. Setelah pengguna terotentikasi, maka pengguna akan mendapatkan hak akses kedalam jaringan kabel internal dan ke internal (dengan menggunakan *proxy server*). Pengguna *Wireless LAN* menggunakan *Web Proxy* dengan protokol SSL dalam proses otentifikasi, memberikan perlindungan keamanan terhadap pencurian informasi *wireless username* dan *password* karena data-data tersebut ditransmisikan dalam bentuk terenkripsi. Proses koneksi *wireless user* dapat dilihat pada gambar 9.

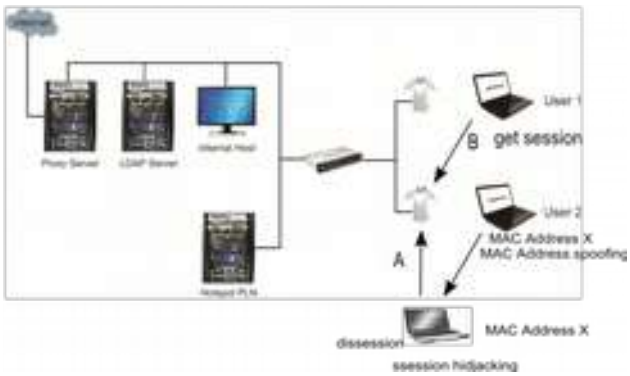


Gambar 9. Proses Koneksi Wireless LAN

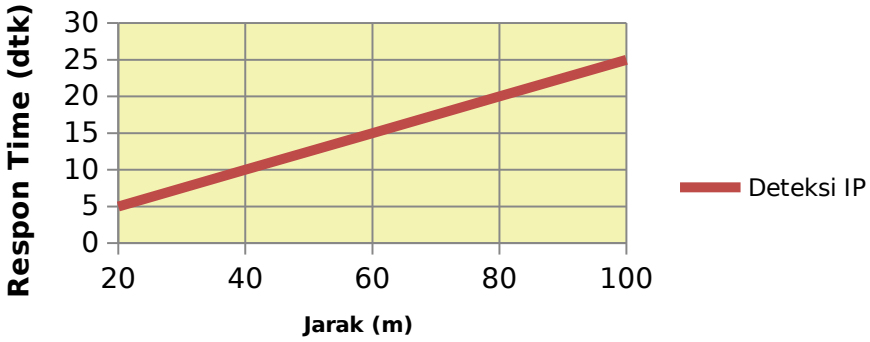
Proses koneksi Wireless yang terjadi adalah sebagai berikut :

- *Wireless user* melakukan proses koneksi dengan *access point* dengan menggunakan *open system authentication* (tanpa menggunakan WEP).
- *Access point* melakukan akses kontrol terhadap permintaaan koneksi dari *wireless user* dengan melakukan *query* ke *hotspot* berdasarkan informasi *MAC Address* yang dimiliki oleh *wireless user*.
- *Query* yang diterima oleh *hotspot* diteruskan ke *server* untuk mendapatkan informasi apakah *MAC Address* dari *wireless user* merupakan *device* yang sudah terdaftar.
- *Server* memberikan konfirmasi apakah *MAC Address* terdapat didalam *database* atau tidak.
- *Hotspot* tersebut menerima informasi dari *server* dan kemudian memberikan konfirmasi proses asosiasi diterima atau tidak berdasarkan informasi tersebut, yaitu apabila *MAC Address* sudah terdaftar maka proses asosiasi diterima dan demikian sebaliknya.
- *Access point* memberikan konfirmasi ke *wireless user* bahwa proses asosiasi telah berhasil dilakukan atau tidak.
- Apabila proses asosiasi berhasil, akan dilakukan proses-proses berikutnya (proses ke tujuh dan seterusnya).
- Setelah *wireless user* mendapatkan sebuah *IP address*, diperlukan suatu proses otentifikasi untuk memastikan bahwa *wireless user* merupakan pengguna yang memang mempunyai hak akses. Untuk itu, *wireless user* harus memasukan informasi berupa *wireless username* dan *password* melalui *Web Proxy* yang menggunakan protokol SSL. Dimana data-data yang ditrasnsmisikan akan dienkripsi sehingga mencegah kemungkinan penyerang dapat mengetahui identitas rahasia dari *wireless user.*
- *Server* memberikan respon apakah proses otentifikasi diterima atau tidak dengan memeriksakan apakah kombinasi *wireless username* dan *pasword* terdapat dalam direktori *database*.

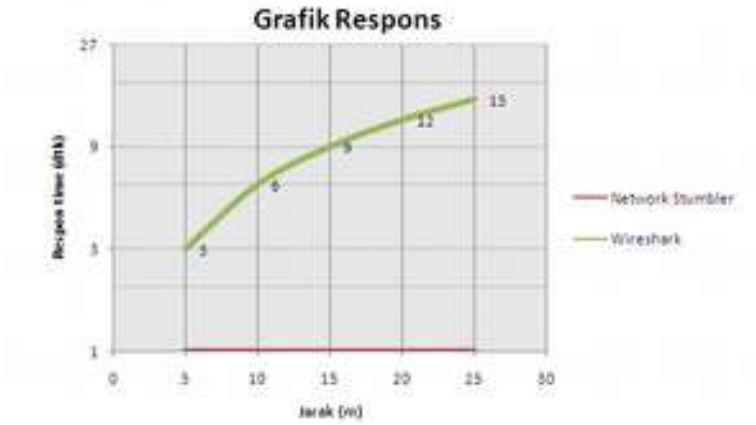
Protokol-protokol tersebut menyediakan otentifikasi, enkripsi dan integritas daya yang tangguh. Protokol yang lain terdapat dilapisan atas (*application layer*) seperti HTTP, FTP dan *telnet* bukan merupakan protokol yang aman karena semua data yang ditransmisikan merupakan *text* biasa. Implementasi jaringan *Wireless LAN* dilingkungan PT. PLN (PERSERO) WILAYAH P2B tidak menggunakan keamanan lapisan *data link layer* (seperti WEP dan WPA), karena itu transmisi data dari protokol yang “tidak aman” tersebut tetap ditransmisikan dalam bentuk *text* biasa (*clear text*). Hal ini berarti titik kelemahan dalam keamanan yang dapat dimanfaatkan penyerang untuk menyadap transmisi data tersebut dan mencoba untuk melakukan serangan terhadap otentifikasi dan akses kontrol dari sistem *WebProxy* di PT. PLN (PERSERO) WILAYAH P2B. Serangan dilakukan adalah *session hijacking*, yaitu serangan yang dilakukan untuk mencuri *session* dari seorang *wireless user* yang sudah terotentifikasi dengan *access point*. dapat dilihat pada Gambar 10.



Gambar 10. *Session Hidjacking* pada *Wireless LAN* dengan *Web Proxy*




Gambar 11. *Hasil percobaan serangan Pendeteksian IP Address*



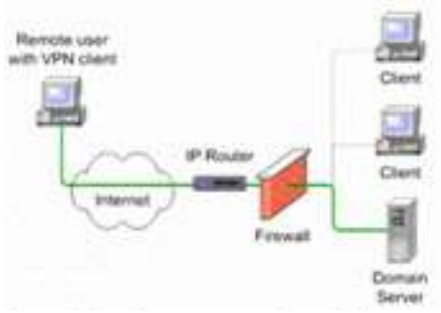

Gambar 12. Grafik Respons Time terhadap Protokol *Wep Proxy*.

Dari grafik Respons Time terlihat bahwa Network Stumbler yang paling cepat mendeteksi sistem keamanannya sedangkan Wireshark yang paling lambat.

**Serangan pada *Virtual Private Network***

Melakukan percobaan serangan terhadap *hotspot* yang menggunakan keamanan ***Virtual Private Network*** dengan berusaha memecahkan *wireless username dan password* dengan jarak yang berbeda dan percobaan untuk mencari *session* koneksi. Dari percobaan yang dilakukan menggunakan *software aircrack* penulis hanya dapat mengidentifikasikan atau memonitor konfigurasi keberadaan *hotspot* tanpa bisa memecahkan *wireless username* dan *password* yang dimiliki *wireless user* asli (Gambar 4.8). Penulis juga hanya bisa mengetahui *IP Address wireless user* asli tanpa bisa merubah *IP Address wireless user* asli.

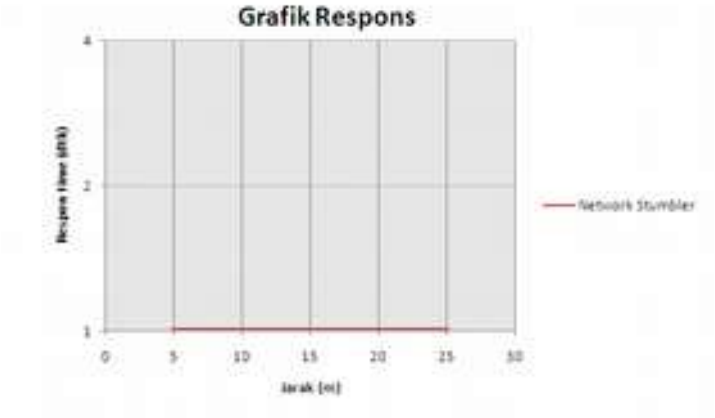
.




Gambar 13. Struktur Jaringan Keamanan dengan VPN

**Tabel 4. Hasil Percobaan Serangan terhadap Protokol VPN**

| Jarak (m) | Network Stumbler | Aircrack | Wireshark |
|---|---|---|---|
| | Respon time rata2 (detik) | Respon time rata2 (detik) | Respon time rata2 (detik) |
| 5 | 0 | Tidak berhasil | Tidak berhasil |
| 10 | 0 | Tidak berhasil | Tidak berhasil |
| 15 | 0 | Tidak berhasil | Tidak berhasil |
| 20 | 0 | Tidak berhasil | Tidak berhasil |
| 25 | 0 | Tidak berhasil | Tidak berhasil |




Gambar 14. Grafik Respons Time terhadap Protokol *VPN*.

**Kesimpulan dan Saran**

Dari hasil penelitian dan percobaan pada Wireless LAN dapat disimpulkan sebagai berikut :

1. Penggunaan keamanan dengan protokol WPA, Web Proxy dan Virtual Private Network (VPN) kurang memberikan perlindungan keamanan dari Network Stumbler.
2. Penggunaan protokol dengan WPA maka respon time rata-rata untuk Network Stumbler lebih cepat dari Wireshark sedangkan Aircrack respon time rata-rata 45 menit untuk jarak 25 m.
3. Penggunaan protokol dengan Web Proxy maka respon time rata-rata untuk Network Stumbler lebih cepat dari Wireshark sedangkan Aircrack tidak berhasil.
4. Penggunaan protokol dengan VPN maka respon time rata-rata untuk Network Stumbler lebih cepat sedangkan respon time rata-rata Wireshark dan Aircrack tidak berhasil.
5. Sistem keamanan dengan menggunakan Protokol VPN lebih baik dibandingkan dengan menggunakan Protokol Web Proxy atau WPA.
6. Untuk kegiatan penelitian selanjutnya, penulis menyarankan untuk melakukan penelitian protokol lain terhadap Network Stumbler.

**Daftar Pustaka**

[1] Stallings, William. 2003. *Cryptography and Network Security*. New Jersey: Prentice Hall.

[2] Edney, Jon and William A. Arbaugh E.2004. *Real8002.11 Security: WiFi Protrcted Access and 802.11i.* Boston: Addison Wesley

[3] Arbough, William A, Narendar Shankar and Y.C Justine Wan, 2001. *Your 802.11 Wireless Network Has No Clothes.* Departemen of Computer Science University of Maryland. 22 September 2004

[4] McNair, Bruce,2002. *Information System Security.* Stevens Institute of Technology. 18 Desember 2004. http://www.ece.stevens-tech.edu/-bmcnair/information_system_ security-F02/class_1.pdf

[5] Borisov, Nikita, Ian Golberg and David Wagner. 2001. *Intercepting Mobile Communication*: *The Insecurity of 802.11*. *5* Oktober 2004.

[6] Schneier, Bruce.1999. *Attack Trees: Modeling Security threats.* Dr. Dobb's Journal December 1999. 18 Desember 2004 http://www.schneier.com/paper-attacktrees-ddj-ft.html

[7] Pervaiz Mohammad O, et all. Security In Wireless Local Area Networks, *Department of Computer Science &Engineering, Florida Atlantic University 777 Glades Road, Boca Raton, Florida 33431,USA*

[8] Glendinning, Ducan. 2003. *802.11 Security.* Intel Corporation. 5 Oktober 2004 http://www.intel.com/idf/us/fall2003/presentations/ FO3USMOB169_OS.Pdf

[9] Borisov, Nikita, Ian Golberg and David Wagner, 2001. *Analisis of 802.11 Security orWired Equivalent Privacy Isn't.* 22 September 2004 http://www.isaac.cs.berkeley.edu/isaac/wep-slides.pdf

[10] He Changhua, John C Mitchell. *Security Analysis and Improvements for IEEE 802.11i*, Electrical Engineering and Computer Science Departments Stanford University, Stanford CA 94305

[11] Al Naamany Ahmed M., Ali Al Shidhani, Hadj Bourdoucen. May 2003. *IEEE 802.11 Wireless LAN Security Overview* . IJCSNS International Journal of Computer Science and Network Security, VOL.6 No.5B, Department of Electrical and Computer Engineering – Sultan Qaboos University, Oman.

[12] WIR01 Wiryana, I Made, (2000b). *Jangan anggap enteng virus.* http://www.pandu.dhs.org/Security/artikel-02