# Evaluasi Keamanan Akses Jaringan Komputer Nirkabel (Kasus : Kantor Pusat Fakultas Teknik Universitas Gadjah Mada)

Ida Bagus Verry Hendrawan Manuaba[1], Risanuri Hidayat[2], Sri Suning Kusumawardani[3]

***Abstract*— The growth of current wireless networks has increased rapidly. The growth of information technology and telecommunications technology requires interoperability, joint regulation and various solutions to solve the increasingly complex problems, such as computer network security issues on wireless networks. An evaluation is needed to maintain and re-assess the stability of the network to remain adequate. This research resulted a model as a result of evaluation that can be used as a useful recommendations to improve the security of a wireless computer network access which affects the performance on the network at the Headquarters of Engineering Faculty of Gadjah Mada University.**

***Intisari*— Perkembangan jaringan nirkabel saat ini telah bertamabvdengan pesat. Perkembangan teknologi informasi membutuhkan kemampuan bekerja sama, pengaturan bersama dan variasi solusi untuk memecahkan masalah rumit yang semakin bertambah, seperti persoalan keamanan jaringan komputer dalam jaringan nirkabel. Sebuah penilaian dibutuhkan untuk memelihara dan menilai ulang stabilitas jaringan agar tetap memadai. Penelitian ini menghasilkan sebuah model sebagai hasil dari penilaian yang dapat digunakan sebagai anjuran berguna untuk meningkatkan keamanan akses jaringan komputer nirkabel yang mempengaruhi kinerja pada jaringan Kantor Pusat Fakultas Teknik Universitas Gadjah Mada.**

***Kata Kunci*— evaluation, wireless, network performance, wireless computer network model.**

## I. PENDAHULUAN

Jaringan komputer telah mengalami perkembangan yang pesat. Seiring dengan meningkatnya kebutuhan pengguna komputer yang terkoneksi ke dalam sebuah jaringan komputer, dibutuhkan juga infrastruktur yang dapat mengakomodir permintaan dari pengguna dan pemberdayaan resource yang tersedia.

Universitas Gadjah Mada telah banyak memanfaatkan teknologi jaringan komputer. Penggunaan teknologi jaringan ini dilakukan untuk mendukung kegiatan perkuliahan serta kegiatan yang berhubungan dengan administrasi pada instansi-instansi yang berada di lingkungan Universitas Gadjah Mada. Kantor Pusat Fakultas Teknik, segala macam proses baik itu layanan yang dibagikan kepada mahasiswa hingga proses administrasi kini menggunakan jaringan komputer. Karena itu semua informasi yang dikirmkan melalui jaringan komputer perlu untuk mendapat suatu perhatian. Jaringan nirkabel yang kaya akan sorotan mengenai keamanannya, perlu untuk mendapatkan perhatian serius. ini dikarenakan jaringan nirkabel memanfaatkan gelombang radio yang dipancarkan secara broadcast, dan bergerak bebas di udara yang dapat ditangkap oleh siapapun.

Perencanaan, perancangan, dan implementasi suatu topologi jaringan, dalam hal ini adalah jaringan komputer nirkabel, tidak dapat dihentikan dengan begitu saja atau dengan kata lain tidak dapat dihandalkan begitu saja. Diperlukan suatu proses lanjutan untuk melakukan suatu penetrasi terhadap kemampuan jaringan tersebut agar tetap sesuai dengan tujuan perancang. Dibutuhkan evaluasi terhadap ketersediaan, kerahasiaan, dan integritas pada jaringan, agar performansi dari jaringan tersebut dapat tetep dihandalkan. Dengan melakukan evaluasi, dapat diketahui celah-celah keamanan yang ada di sistem jaringan komputer nirkabel yang sedang berjalan sehingga dapat dibuat suatu model sistem keamanan jaringan komputer nirkanbel yang baik.

## II. *WIRELESS LOCAL AREA NETWORK (WLAN)*

*Wireless Local Area Network* adalah sistem komunikasi yang fleksibel dimana pengirim dan penerimaan datanya melalui media udara dengan menggunakan teknologi frekuensi radio. WLAN dapat digolongkan menjadi dua kategori utama yakni:

### *A. WLAN berbasis Ad-Hoc*

Pada model jaringan yang berbasis ad-hoc, jaringan antara satu perangkat dengan perangkat yang lain dilakukan secara spontan/langsung tanpa melalui konfigurasi tertentu selama signal dari pemancar yakni transmitter dapat diterima dengan baik oleh perangkat-perangkat penerima yakni receiver.

### *B. WLAN berbasis Infrasturkur*

Pada model jaringan yang berbasis infrastruktur, model ini, untuk memberikan koneksi antara perangkat yang terhubung kedalam jaringan WLAN, diperlukan suatu intermediary device berupa access point yang terhubung dalam jaringan komputer kabel, sebelum melakukan transmisi kepada perangkat-perangkat penerima signal.

Kerentanan jaringan WLAN terhadap keamanan data, informasi, dan ketersediaan layanan menjadi topik yang tidak henti-hentinya menjadi sorotan dan perbincangan. Untuk itu, dikemukakan suatu teori bahwa suatu jaringan komputer dikatakan aman apabila

1) *Privacy* & *Confidentiality:* Merupakan suatu mekanisme yang yang dilakukan untuk melindungi suatu informasi dari pengguna jaringan yang tidak memiliki hak, sedangkan confidentiality lebih mengarah kepada tujuan dari informasi yang diberikan dan hanya boleh untuk tujuan tersebut saja.

[1] *Teknik Elektro dan Teknologi Informasi Fakultas Teknik Universitas Gadjah Mada Jln. Grafika 2 Yogyakarta 55281 INDONESIA (e-mail:* verry.manuaba@mti.gadjahmada.edu).

[2, 3] *Jurusan Teknik Elektro dan Teknologi Informasi Fakultas Teknik Universitas Gadjah Mada, Jln. Grafika 2 Yogyakarta 55281 INDONESIA (e-mail:* risanuri@*te.ugm.ac.id)*

2) *Integrity:* Merupakan aspek yang mengutamakan akses informasi yang ditujukan untuk pengguna tertentu, dimana integritas dari informasi tersebut masih terjaga.

3) *Authentication:* Aspek ini mengutamakan validitas dari user yang melakukan akses terhadap suatu data, informasi, atau layanan dari suatu institusi.

4) *Availability:* Merupakan aspek yang berhubungan dengan ketersediaan data, informasi, atau layanan, ketika data, informasi atau layanan tersebut diperlukan.

5) *Access Control:* Dimana aspek ini berhubungan dengan klasifikasi pengguna dan cara pengaksesan informasi yang dilakukan oleh pengguna.

6) *Non Repudiation:* Merupakan aspek yang berkaitan dengan pencatatan pengguna, agar pengguna data, informasi atau layanan tidak dapat menyangkal bahwa telah melakukan akses terhadap data, informasi, ataupun layanan yang tersedia [1].

Sorotan akan keamanan pada jarinan WLAN dititik beratkan pada faktor keamanan dari media wireless pada tipe jaringan ini. Banyak serangan yang dapat terjadi pada jaringan dengan media wireless. Serangan-serangan yang paling sering muncul pada jaringan ini adalah sebagai berikut.

1) *Reveal SSID:* Merupakan serangan yang dilakukan dengan menyingkap SSID dari access point yang sengaja disembunyikan oleh administrator jaringan komputer.

*2*) *MAC Address Spoofing:* Merupakan usaha yang dilakukan oleh seorang hacker untuk menembus keamanan MAC address filtering dengan melakukan spoofing MAC address pada jaringan komputer, dengan menggunakan MAC address user sah untuk mendapatkan layanan jaringan komputer.

3) *Authentication Attack:* Merupakan serangan terhadap authentication user yang sah, sehingga menyebabkan kelumpuhan atau disconnectnya user sah. Attacker memanfaatkan serangan ini afar mendapatkan resource yang lebih dalam menggunakan layanan jaringan.

4) *Eavesdropping:* Merupakan serangan yang dilakukan dengan cara mendengarkan semua paket-paket yang ditransmisikan oleh user yang berada dalam jaringan 14 komputer yang tidak terenkripsi menggunakan teknik enkripsi apapun.

5) *Session Hijacking:* Merupakan suatu serangan yang menyerang suatu sesi seorang pengguna untuk dimanfaatkan sebagai ajang untuk mendapatkan suatu hak akses ke layanan yang sedang diakses oleh user sah.

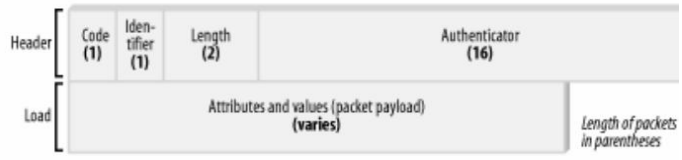
6) *Man In The Middle Attack:* Merupakan serangan yang dilakukan dengan melakukan spoofing terhadap user sah sehingga transmisi yang dilakukan target adalah menuju attacker, sehingga attacker mendapatkan semua informasi yang di transmisikan oleh target.

7) *Denial of Service:* Merupakan serangan yang menyerang ketersedian sumber daya sehingga menyebabkan user sah mengalami discconet dari jaringan komputer.

8) *Rogue Access Point:* Merupakan serangan yang menggunakan suatu perangkat access point yang dibuat sama dengan access point yang berada pada suatu institusi. Sehingga ketika user sah melakukan akses ke access point ini.

## III. *REMOTE AUTHENTICATION DIAL IN USER SERVICE (RADIUS)*

Server Otentikasi merupakan perangkat keamanan pada suatu jaringan komputeryang menerapkan proses otentikasi untuk melayani permintaan otentikasi dari pengguna layanan jaringan. Server otentilkasi ini menerapkan model AAA (*authentication, authorization,* dan *accounting*). *Authentication* merupakan proses pengesahan identitas pelanggan (end-user) untuk mengakses jaringan. *Authorization* merupakan merupakan proses pengecekan wewenang yang dimiliki oleh pelanggan pengguna jaringan komputer. Sedangkan *accounting* merupakan proses penghitungan yang dilakukan oleh sistem yang kemudian melakukan pencatatan sumberdaya yang telah dipakai oleh pengguna jaringan komputer nirkabel. RADIUS memiliki suatu format paket yang digunakan dalam melakukan transmisi data.




Gbr. 1 Protokol RADIUS

1) *Code:* Code pada protokol RADIUS terdiri dari 8 bit yang menunjukan tipe paket RADIUS dengan nilai sebagai berikut.

TABEL I
*CODE* PADA PROTOKOL RADIUS

| Nilai | Deskripsi |
|---|---|
| 1 | *access – request* |
| 2 | *access – accept* |
| 3 | *access – reject* |
| 4 | *accounting – request* |
| 5 | *accounting – respond* |
| 11 | *access challenge* |
| 12 | *status – server* |
| 13 | *status – client* |
| 255 | *Reserved* |

2) *Identifier:* Identifier terdiri atas 8 bit yang digunakan untuk memberikan identifikasi pada paket permintaan client dan paket respon yang diberikan oleh server RADIUS.

3) *Length:* length terdiri dari 16 bit yang menginfromasikan panjang dari paket termasuk didalmnya code, identifier, length, authenticator, attribute.

4) *Authenticator:* authenticator terdiri dari 128 bit. Most Significant Bit (MSB) merupakan nilai yang pertama kali dikirimkan. Sedangkan nilai lainya digunakan untuk algoritma *password hiding.* Pada paket

*access-request* nilai *authenticator* yang berupa bilangna acak ini dinamakan request

5) *Authenticator:* Nilai ini berisi one way hash MD5 yang dihasilkan dari proses penyandian serangkaian bit-bit pada paket RADIUS yang dapat dituliskan sebagai berikut ResponseAuth = MD5 (Code + ID + Length + RequestAuth + Attributes + Secret)

6) *Attributs:* Bagian paket ini berisi otentikasi, otorisasi, informasi dan detil konfigurasi spesifik yang diperlukan untuk permintaan dari client RADIUS ataupun NAS.

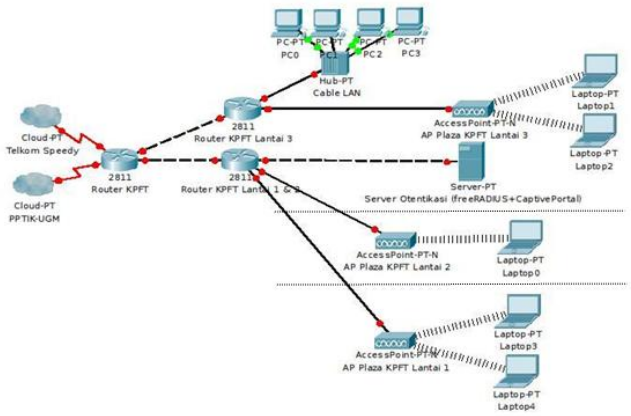
Dalam penerapanya, RADIUS dipadukan dengan captive portal yang merupakan suatu teknik routing traffic untuk melakukan otentikasi dan pengamanan data yang melewat network internal ke network eksternal dengan membelokan traffic pengguna ke sebuah halaman login, ini dilakukan agar

## III. METODE EVALUASI JARINGAN

Mekanisme evaluasi keamanan jaringan komputer nirkabel pada KPFT-UGM dilakukan dengan cara membangun jaringan simulasi jaringan komputer nirkabel KPFT-UGM dengan mensimulasikan substansi - substansi keamanan jaringan yang terdapat pada KPFT-UGM. Pengujian yang dilakukan pada jaringan simulasi, dilakukan dengan melakukan penetration test dengan menyerang jaringan simulasi dengan menggunakan serangan-serangan yang mungkin muncul pada jaringan komputer nirkabel yang sesuai pada studi kasus. Serangan sesuai untuk jaringan simulasi tersebut adalah MAC address spoofing, authentication attack, denial of service, eavesdropping, man in the middle attack, dan WEP cracking. Hasil dari penetration testing mendapatkan suatu hasil yang dapat dianalisis dan dievaluasi untuk mendapatkan suatu model keamanan jaringan komputer nirkabel yang digunakan untuk menutup celah-celah keamanan jaringan komputer nirkabel KPFT-UGM, yang dilanjutkan dengan melakukan pengujian terhadap model yang telah dibuat untuk memastikan model yang digunakan tepat.

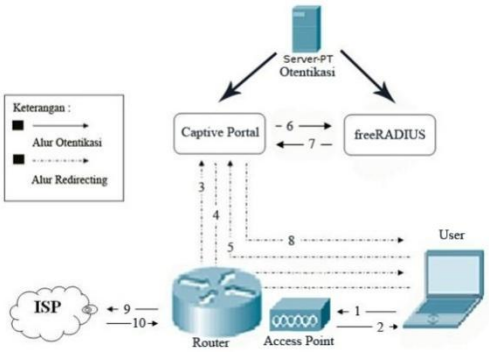
## IV. SIMULASI JARINGAN KPFT-UGM

Untuk melakukan simulasi terhadap jaringan komputer nirkabel KPFT-UGM, dibutuhkan topologi jaringan yang sesuai untuk menggambarkan keadaan jaringan pada studi kasus.



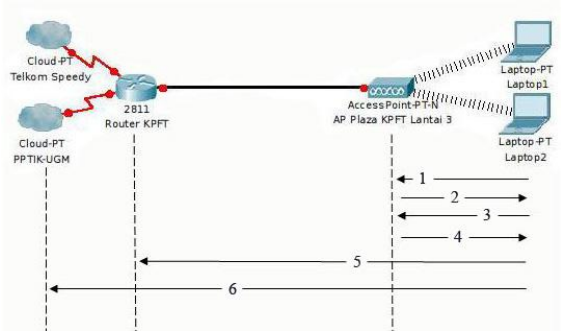

Gbr. 2 Topologi Jaringan Komptuer KPFT-UGM

Pada Gbr. 2 merupakan topologi pada jaringan komputer KPFT UGM yang mana terdapat dua buah model keamanan yang berbeda. Model yang pertama yakni model pada KPFT-UGM untuk lantai 1 dan 2 menggunakan mekanisme keamanan dengan server otentikasi RADIUS dengan menggunakan captive portal untuk meredirect user ke halaman otentikasi.




Gbr. 3 *Model Keamanan KPFT-UGM Lantai 1&2*

Sedangkan model keamanan pada KPFT-UGM lantai 3 menggunakan mekanisme otentikasi yang menggunakan WEP sebagai metode keamanan jaringan komputer nirkabelnya.




Gbr. 4 *Model keamanan KPFT Lantai 3*

Pada Gbr. 3 dan 4 terdapat mekansime otentikasi yang diwakilkan oleh penomoran yang tertera pada gambar untuk menunjukan mekanisme otentikasi yang diberlakukan pada setiap partisi yang ada di KPFT-UGM.

Setelah mendapatkan informasi menganai mekanisme keamanan jaringan komputer nirkabel pada KPFT-UGM, berikutnya merancang konfigurasi untuk server RADIUS yang dipadukan dengan captive portal. Konfigurasi yang diruning ketika captive portal dan RADIUS dijalankan dapat dilihat pada file `/etc/chilli/main.conf`

```
domain lan
dns1 202.3.208.11
uamhomepage http://10.1.0.1/coova_json/splash.php
wisprlogin https://coova.org/app/uam/auth
wwwdir /etc/chilli/www
wwwbin /etc/chilli/wwwsh
locationname "KPTU-Simulasi"
RADIUSlocationname KPTU_Simulasi
RADIUSlocationid isocc=,cc=,ac=,network=KPTUFT
```


Gbr. 5 *Captive Portal*

## V. PENGUJIAN DAN ANALISIS

Vulnerability assessment dilakukan untuk menilai kerentanan jaringan komputer nirkabel yang dilakukan oleh seorang pengguna untuk menilai dan mengukur tingkat keamanan yang digunakan pada suatu jaringan. Test yang dilakukan pada jaringan simulasi ini menggunakan metode penetration test untuk mengetahui celah keamanan yang ada pada jaringan KPFT-UGM yang dilakukan pada simulasi jaringan komputer pada KPFT-UGM.

TABEL II
*PENETRATION TESTING* PADA KPFT-UGM LANTAI 1&2

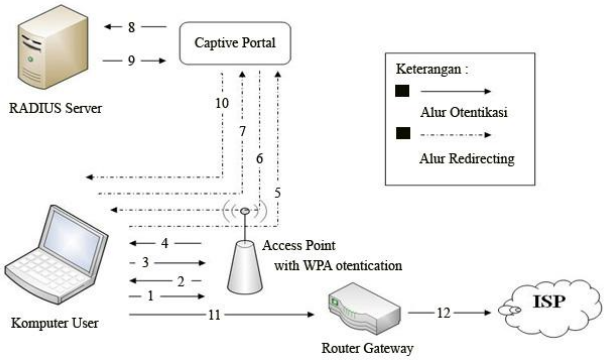
| Jenis Serangan | Informasi Yang Dibutuhkan | Status Serangan |
|---|---|---|
| MAC *Address* Spoofing | List MAC *Address user* yang terkoneksi ke dalam jaringan. | Berhasil |
| Authentication Attack Tunggal | List MAC *Address user* yang terkoneksi ke dalam jaringan, channel yang digunakan oleh *Access point* | Berhasil |
| Denial of Service | List IP *address* dari *user* yang terkoneksi ke dalam jaringan | Berhasil |
| Eavesdropping | *Attacker* harus berada dalam Jaringan Intranet | **Gagal** |
| Man In The Middle Attack | Port yang terbuka pada Server, IP *address* dari *user* yang terkoneksi ke dalam jaringan | **Gagal** |

Pada Tabel 2, merupakan serangan yang dilakukan pada KPFT-UGM lantai 3 yang menunjukan bahwa serangan eavesdropping dan Man In the Middle Attack gagal terjadi pada jaringan yang menggunakan RADIUS authtentication server.

TABEL III
*PENETRATION TESTING* PADA KPFT-UGM LANTAI 3

| Jenis Serangan | Informasi Yang Dibutuhkan | Status Serangan |
|---|---|---|
| WEP Cracking | Channel yang digunakan oleh *Access point*, MAC *address* atau SSID dari *access point* | Berhasil |

Keberhasilan serangan WEP cracking, dapat menembus mekanisme keamanan yang terdapat pada lantai 3 KPFT-UGM. Dari serangan-serangan yang telah dilakukan dengan penetration testing, dapat dihasilkan suatu analisis bahwa dibutuhkan suatu lapisan keamanan untuk mencegah user yang tidak memiliki hak, agar tidak dapat bergabung dengan jaringan. Lapisan keamanan yang dibutuhkan yakni berupa otentikasi pada layer 2, yang terdapat pada access point yakni berupa suatu lapisan yang menggunakan teknologi ekripsi. Sejauh ini, teknik otentikasi ini ada tiga macam, seperti yang telah disebutkan pada bab sebelumnya, yakni WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access), dan WPA2 (Wi-Fi Protected Access2). Penggunaan WEP tidak memberikan hasil yang baik, dikarenakan mekanisme otentikasi dengan menggunakan WEP masih dapat dengan mudah diretas dengan menggunakan software peretas aircrack. Rekomendasi yang disarankan adalah menggunakan mekanisme ontentikasi yang lebih baik, yakni dengan menggunakan WPA/WPA2. Rekomendasi yang disarankan tersebut dipadukan dengan server otentikasi RADIUS untuk memberikan mekanisme keamanan jaringan komputer nirkabel yang berlapis.




Gbr. 6 *Model Keamanan Jaringan KomputerNirkabel KPFT-UGM*

Perancangan model keamanan jaringan komputer nirkabel menggunakan dua lapisan keamanan yakni menggunakan WPA dan menggunakan server otentikasi RADIUS yang dikombinasikan dengan mengguanak captive portal. Captive portal akan melakukan redirecting pengguna ke halaman otantikasi ketika pengguna melakukan akses ke jaringan internet dengan menggunakan web browser. Captive portal akan berasosiasi dengan server RADIUS untuk melakukan validitas dari username dan password yang dikirimkan oleh pengguna.

Selain memberikan tingkat keamanan yang lebih baik, penggunaan RADIUS yang dirancang sesuai model AAA (*authentication, authorization,* dan *accounting*) memberikan kemudahan dalam melakukan pencatatan aktivitas pengguna. Untuk menguji model keamanan jaringan komputer nirkabel ini, dilakukan dengan teknik yang sama yakni serangan-serangan yang mungkint terjadi pada jaringan komputer nirkabel, yakni

TABEL IV
PENGUJIAN MODEL KEAMANAN JARINGAN KOMPUTER NIRKABEL KPFT-UGM

| Jenis Serangan | Informasi Yang Dibutuhkan | Status Serangan Pada Model |
|---|---|---|
| MAC *Address* Spoofing | List MAC *Address user* yang terkoneksi ke dalam jaringan. | **Gagal** |
| Denial of Service | List IP *address* dari *user* yang terkoneksi ke dalam jaringan | **Gagal** |
| Man In The Middle Attack | Port yang terbuka pada Server, IP *address* dari *user* yang terkoneksi | **Gagal** |
| Eavesdropping | *Attacker* harus berada dalam Jaringan Intranet | **Gagal** |
| Cracking WPA | Dictionary Word, handshake *user* lain, BSSID dari *access point*. | **Gagal** |

## VI. KESIMPULAN

Kesimpulan yang dapat diberikan dari hasil penelitian ini adalah evaluasi terhadap jaringan komputer nirkabel pada KPFT-UGM dilakukan dengan melakukan penetration testing berupa MAC address spoffing, authentication attack, DoS, MITM, Eavesdropping, WEP cracking. Penggunaan sistem otentikasi dengan menggunakan server otentikasi yang dipadukan dengan captive portal belum cukup handal untuk menangani serangan denial of service, authentication attack, dan MAC address spoofing. Model keamanan yang menggunakan kombinasi antara server otentikasi, captive portal, firewall, serta WPA/WPA2 yang dihasilkan pada penelitian ini dapat menutup celah keamanan dan meningkatkan mekanisme keamanan jaringan nirkabel. Penggunaan sistem otentikasi dengan menggunakan server otentikasi yang dipadukan dengan captive portal belum cukup handal untuk menangani serangan denial of service, authentication attack, dan MAC address spoofing. Penggunaan password otentikasi disarankan untuk menggunakan password yang mengkombinasikan angka, huruf dan karakter untuk meningkatkan keamanan dari password yang digunakan.

## REFERENSI


[1] Garfinkel, S; Spafford, G; Schwartz, A. 2003. *Practical UNIX and Internet Security (Third Edition)*. O'Reilly & Associate Inc. Sebastopol, CA.

[2] Lukas J. 2006. *Jaringan Komputer*. Yogyakarta. Penerbit Graha Ilmu.

[3] Lyon. G. Nmap official site. http://nmap.org/ diakses pada Selasa tanggal 8 Maret 2011 pada pukul 10.25

[4] Nugroho, M. A. 2001. *Studi Kasus Celah Keamanan Pada Jaringan Nirkabel Yang Menerapkan WEP (Wired EquivalentPrivacy)*. STMIK AMIKOM Yogyakarta.

[5] Ramadhani, Erika. 2010 *Analisa Keamanan Jaringan Nirkabel di Universitas Gadjah Mada Dengan Menggunakan Metode Wardriving*. Yogyakarta. Magister Teknologi Informasi Universitas Gadjah Mada.

[6] Sadikin, M. F. 2008. *Analisis Kinerja Infrastuktur Jaringan KomputerTeknik Elektro UGM*. Yogyakarta. Magister Teknologi Informasi Universitas Gadjah Mada.

[7] Santika, M. E. 2005. *Arsitektur Untuk Mengamankan Jaringan Nirkabel*. Jakarta, PT. Bank Bukopin.

[8] Sarjanoko, R. J. 2007. *Analisis Keamanan Nirkabel Local Area Network Standard 802.11 : Kasus PT. Masterdata Jakarta*. Bogor, Sekolah Pascasarjana Institut Pertanian Bogor.

[9] Setiawan. M. A., Febyatmoko. G. S., 2006. *Sistem Autentikasi, Otorisasi, dan Pelaporan Koneksi User Pada Jaringan Wireless Menggunakan Chilli Spot dan Server RADIUS*. Yogyakarta. Seminar Nasional Aplikasi Teknologi Informasi (SNATI 2006)

[10] Sharpe. R, Lamping. U, dkk. 2004. *Wireshark User Guides : 36153 for Wireshark 1.5*. http://www.wireshark.org/ diakses pada Selasa, 8 Maret 2011 pada pukul 09.13

[11] Suryadana, Y. 2010 *Analisis Kemanan Jaringan Internet (Studi Kasus : Pemerintah Provinsi Kalimantan Timur)*. Yogyakarta. Magister Teknologi Informasi Universitas Gadjah Mada Yogyakarta.

[12] Triyoga, A. 2004. *Analisis dan Perancangan Jaringan Nirkabel Studi Kasus Magister Teknologi Informasi Universitas Gadjah Mada*. Magister Teknologi Informasi Universitas Gadjah Mada.