AUDIT KEAMANAN JARINGAN *WIRELESS* MENGGUNAKAN *WIRELESS SECURITY CHECKLIST* ISO 27001 STUDI KASUS DI BPKB DIKPORA PROVINSI DIY

Skripsi

Untuk memenuhi sebagai persyaratan

Mencapai derajat Sarjana S-1

Di susun oleh:

Andhika Danawiputra

(NIM: 06650038)

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA

YOGYAKARTA

2011

Universitas Islam Negeri Sunan Kalijaga **FM-UINSK-BM-05-07/R0**

PENGESAHAN SKRIPSI/TUGAS AKHIR

Nomor : UIN.02/D.ST/PP.01.1/1197/2011

Skripsi/Tugas Akhir dengan judul	:	Audit Keamanan Jaringan Wireless Menggunakan Wireless Security Checklist ISO 27001 Studi Kasus di BPKB Dikpora Provinsi DIY
Yang dipersiapkan dan disusun oleh	:	
Nama	:	Andhika Danawiputra
NIM	:	06650038
Telah dimunaqasyahkan pada	:	27 Juni 2011
Nilai Munaqasyah	:	A / B

Dan dinyatakan telah diterima oleh Fakultas Sains dan Teknologi UIN Sunan Kalijaga

TIM MUNAQASYAH :

Ketua Sidang

Landung Sudarmana, M.Kom
NIY. 0527027001

Penguji I

Sumarsono, S.T, M.Kom
NIP.19710209 200501 1 003

Penguji II

M. Didik R. Wahyudi, S.T, M.T
NIP. 19760812 200901 1 015

Yogyakarta, 1 Juli 2011
UIN Sunan Kalijaga
Fakultas Sains dan Teknologi
Dekan

Prof. Drs. H. Akh. Minhaji, M.A, Ph.D
NIP. 19580919 198603 1 002

Universitas Islam Negeri Sunan Kalijaga FM-UINSK-BM-05-03/R0

SURAT PERSETUJUAN SKRIPSI/TUGAS AKHIR

Hal : Persetujuan Skripsi / Tugas Akhir
Lamp :

Kepada
Yth. Dekan Fakultas Sains & Teknologi
UIN Sunan Kalijaga Yogyakarta
Di Yogyakarta

Assalamu'alaikum wr. wb.

Setelah membaca, meneliti, memberikan petunjuk dan mengoreksi serta mengadakan perbaikan seperlunya, maka kami selaku pembimbing berpendapat bahwa skripsi Saudara:

Nama : Andhika Danawiputra
NIM : 06650038
Judul Skripsi : Audit Keamanan Jaringan *wireless* menggunakan *wireless security checklist* ISO 27001 Studi Kasus Di BPKB Dikpora Provinsi DIY

sudah dapat diajukan kembali kepada Fakultas Sains & Teknologi Jurusan/ Program Studi Teknik Informatika UIN Sunan Kalijaga Yogyakarta sebagai salah satu syarat untuk memperoleh gelar Sarjana Strata Satu.

Dengan ini kami mengharap agar skripsi/tugas akhir Saudara tersebut di atas dapat segera dimunaqsyahkan. Atas perhatiannya kami ucapkan terima kasih.

Wassalamu'alaikum wr. wb.

Yogyakarta,
Pembimbing I

Landung Sudarmana M.Kom
NIP. 0527027001

Universitas Islam Negeri Sunan Kalijaga FM-UINSK-BM-05-03/R0

SURAT PERSETUJUAN SKRIPSI/TUGAS AKHIR

Hal : Persetujuan Skripsi / Tugas Akhir
Lamp :

Kepada
Yth. Dekan Fakultas Sains & Teknologi
UIN Sunan Kalijaga Yogyakarta
Di Yogyakarta

Assalamu'alaikum wr. wb.

Setelah membaca, meneliti, memberikan petunjuk dan mengoreksi serta mengadakan perbaikan seperlunya, maka kami selaku pembimbing berpendapat bahwa skripsi Saudara:

Nama : Andhika Danawiputra
NIM : 06650038
Judul Skripsi : Audit Keamanan Jaringan *wireless* menggunakan *wireless security checklist* ISO 27001 Studi Kasus Di BPKB Dikpora Provinsi DIY

sudah dapat diajukan kembali kepada Fakultas Sains & Teknologi Jurusan/ Program Studi Teknik Informatika UIN Sunan Kalijaga Yogyakarta sebagai salah satu syarat untuk memperoleh gelar Sarjana Strata Satu.

Dengan ini kami mengharap agar skripsi/tugas akhir Saudara tersebut di atas dapat segera dimunaqsyahkan. Atas perhatiannya kami ucapkan terima kasih.

Wassalamu'alaikum wr. wb.

Yogyakarta,
Pembimbing II

Bambang Sugiantoro S.Si, M.T
NIP. 19751024 200912 1 002

PERNYATAAN KEASLIAN SKRIPSI

Yang bertanda tangan dibawah ini:

Nama : Andhika Danawiputra

NIM : 06650038

Program Studi : Teknik Informatika

Fakultas : Sains dan Teknologi

Menyatakan bahwa skripsi dengan judul **"AUDIT KEAMAMAN JARINGAN *WIRELESS* MENGGUNAKAN *WIRELESS SECURITY CHECKLIST* ISO 27001 STUDI KASUS DI BPKB DIKPORA PROVINSI DIY"** tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta, 20 Juni 2011

Yang menyatakan

METERAI TEMPEL
2EDFEAAF159182481
ENAM RIBU RUPIAH
6000 DJP

Andhika Danawiputra
NIM. 06650038

KATA PENGANTAR

Alhamdulillah, segala puji bagi Allah *Subhanau wa ta'ala* atas limpahan rahmat, hidayah, serta bimbingan-Nya. Shalawat dan salam semoga tercurah kepada Nabi Muhammad *Sholallahu 'alaihi wa sallam*. Akhirnya penulis dapat menyelesaikan penelitian tugas akhir yang berjudul Audit Keamanan Jaringan Wireless Menggunakan *Wireless* Security checklist Standard ISO 27001 Studi Kasus di BPKB DIKPORA DIY. Oleh karena itu, dengan segala kerendahan hati pada kesempatan ini penulis mengucapkan banyak terima kasih kepada:

1. Ayahanda tercinta Drs. Sumanto, S.Pd yang tak jemu-jemu mencurahkan perhatiannya dan motivasi kepada buah hatinya sehingga menghadirkan semangat dalam menjalani proses skripsi ini.
2. Ibunda tercinta Imro'atin, S.Pd yang selalu mencurahkan doa nya di setiap waktu agar semua proses yang dijalani saya berjalan dengan lancan tanpa hambatan.
3. Kakanda tercinta Yukha Kumoratih Primasari, S.E. yang selalu memberikan dukungan agar bisa meraih cita-cita setinggi tingginya dan dapat membangga kan orang tua.
4. Bapak Prof. Drs. H. Akh. Minhaji, M.A, Ph.D selaku Dekan fakultas Sains dan Teknologi UIN Sunan Kalijaga.

5. Bapak Sumarsono, M.Kom, selaku ketua Program Studi Teknik Informatika UIN Sunan Kalijaga.
6. Bapak Landung Sudarmana, M.Kom selaku Dosen Pembimbing I atas bimbingan, arahan dalam penyusunan skripsi.
7. Bapak Bambang Sugiantoro, M.T selaku Dosen Pembimbing II yang telah memberikan saran dan masukkan kepada penulis dalam menyusun skripsi.
8. Para dosen Teknik Informatika UIN Sunan Kalijaga yang telah memberikan banyak bekal ilmu kepada penulis.
9. Saudara Uki Syukri Gozali atas saran, bantuan, bimbingan, serta kesabarannya selama membimbing penulis dalam penyusunan skripsi.
10. Sahabat-sahabatku di kampus UIN tercinta Nurdin, Sigit, Rian, Sunu, Rifqi, Fathan, Ali, Wahid, Mas Aan, Fikri, Imam, Alex, irvan, Sidiq, Arfan, Triawan, teman-teman Teknik Informatika angkatan 2005, 2006, 2007, 2008 yang telah memberkan bantuan, dukungan serta motivasi kepada penulis dalam menyelesaikan penulisan skripsi ini.
11. Sahabat dekatku SMA Mohammad Abdullah Maulana dan Satria Utama trimakasih telah memberi motivasi kepada saya agar skripsi ini cepat selesai.
12. Teman teman kos Ardian Offset Bambang, Fahri, Pipink, Peeqee, Jarwo, Bejo, Sony, Fery, Iwan, Ronel, Yonas dll. Trimakasih doanya semua.
13. Semua pihak yang telah memberikan bantuan dan dukungan kepada penulis dalam penyusunan skripsi yang tidak dapat disebutkan satu per satu. Akhir

kata, semoga Allah *Subhanahu wa ta'ala* memberikan balasan kebaikan atas segala bantuan yang telah diberikan kepada penulis. Amin

Yogyakarta, 24 April 2011

Penulis

HALAMAN PERSEMBAHAN

Halaman ini ku persembahkan untuk:

- ***Sujud syukurku kepada Allah SWT yang telah melimpahkan nikmat, kemudahan, serta hidayahnya.***
- ***Shalawat serta salam kepada nabi besar Muhammad SAW, keluarga, sahabat serta pengikutnya.***
- ***Ibu, Ayah, kakak serta keluargauntuk semua kebaikan, doa dan motivasi serta kasih saying yang tak tergantikan.***
- ***Sahabat-sahabatku, teman belajar, teman futsal Tif 2006: Irvan, Sigit, Fathan, Fikri, Aslam, Arfan, Imam, Alex, Sunu, Ikhsan, Qori, Didi, Ukie, Uzad dll yang belum sempat saya sebutkan, trimakasih atas dukungan dan semangat yang telah di berikan untuku.***
- ***Teman-teman Teknik Informatika 2006, 2007, 2008,yang tidak bisa saya sebutkan satu persatu.***
- ***Teman-teman kos Ardian Ofset tercinta. Terimakasih atas motivasinya.***
- ***Serta orang-orang yang pernah saya temui dalam hidupku, semoga Allah SWT membalas kebaikan kalian semua. Amien.....***

HALAMAN MOTTO

- *Kegagalan hanya terjadi bila kita menyerah (Lessing)*

- *"sesungguhnya Allah tidak akan mengubah nasib suatu kaum kecuali kaum itu sendiri yang mengubah apa-apa yang pada diri mereka (QS Ar-Ra'du: 11)*

- *Jenius adalah 1 % inspirasi dan 99 % keringat. Tidak ada yang dapat menggantikan kerja keras. Keberuntungan adalah sesuatu yang terjadi ketika kesempatan bertemu dengan kesiapan. – (Thomas A. Edison)*

- *Urusan kita dalam kehidupan bukanlah untuk melampaui orang lain, tetapi untuk melampaui diri sendiri, untuk memecahkan rekor kita sendiri, dan untuk melampaui hari kemarin dengan hari ini (Stuart B. Johnson)*

- *Kita bisa bukan hanya karena kita pandai, namun kita bisa karena kita biasa melakukannya (Komang Leo Triandana)*

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

Audit Keamanan jaringan *Wireless* Menggunakan *Wireless Security Checklist* ISO 27001

Studi Kasus di BPKB DIKPORA Provinsi DIY.

Andhika Danawiputra

NIM. 06650038

INTISARI

Teknologi *wireless* menawarkan beragam kemudahan dan kelebihan dibandingkan teknologi kabel yang sudah ada. Dinas Pendidikan DIKOPRA DIY adalah salah satu lembaga yang menerapkan jaringan wireless. Namun teknologi *wireless* memiliki banyak kelemahan dibandingkan dengan jaringan kabel. Hal ini membuat para hacker tertarik mengeksplore kemampuannya dengan melakukan penyerangan terhadap jaringan wireless dengan melakukan aktifitas illegal seperti *sniffing packet, packet injection, illegal authentication*, sampai *cracking* WEP, WPA/WPA2

Wireless Security Checklist ISO 27001 adalah standar keamanan jaringan wireless. Dalam *Wireless Security Checklist* ISO 27001 memuat point-point keamanan jaringan wireless. Dalam Dinas Pendidikan BPKB DIKPORA DIY perlu diadakannya Audit wireless security guna mengetahui sejauh mana tingkat keamanan yang ada pada lembaga tersebut.

Dengan adanya *Audit Wireless security* maka lembaga Dinas Pendidikan DIKPORA DIY mengetahui apa saja yang perlu dibenahi dalam jaringan wireless di lembaga tersebut sesuai dengan kebutuhannya. serta pihak Dinas Pendidikan DIKPORA DIY paham mengenai konsep jaringan wireless.

Kata Kunci: Wireless, Wireless Security, ISO 27001

Wireless Network Security Auditing Wireless Security Using ISO 27001 Checklist Case Studies in BPKB DIKPORA DIY .

Andhika Danawiputra

NIM. 06650038

ABSTRACT

Wireless technologies offer a variety of conveniences and advantages over existing cable technology. Dinas DIKOPRA DIY is one of the institutions that implement a wireless network. But wireless technology has many disadvantages compared to the wired network. This makes the hackers are interested in explore its ability to conduct attacks on wireless networks by conducting illegal activities such aspacket sniffing, packet injection, illegal authentication, until cracking WEP, WPA/WPA2.

Wireless Security Checklist ISO 27001 is a standard wireless network security. In the Wireless Security Checklist ISO 27001 includes a point – point wireless network security. The Education Department needs to the holding of BPKB DIKPORA DIY wireless security audit to determine the extent to which the existing level of security atthese institutions.

With the Wireless security audit the institution DIKPORA DIY Education Department knows what needs to be addressed in a wireless network at the agency in accordance with their needs. And the Department of Education DIKPORA DIY understand the concept of a wireless network security.

Keywords: Wireless, Wireless Security, ISO 27001

BAB I

PENDAHULUAN

1.1 Latar Belakang

Teknologi *wireless* menawarkan beragam kemudahan, kebebasan dan fleksibilitas yang tinggi. Teknologi *wireless* memiliki cukup banyak kelebihan dibandingkan teknologi kabel yang sudah ada. Teknologi *wireless* sangat nyaman untuk digunakan. Pengaksesan Internet bisa dilakukan di posisi mana pun selama masih berada dalam jangkauan *wireless* (Yani, 2008).

Namun, Jaringan *wireless* memiliki lebih banyak kelemahan dibanding dengan jaringan kabel. Saat ini perkembangan teknologi *wireless* sangat signifikan sejalan dengan kebutuhan sistem informasi yang *mobile*. Banyak penyedia jasa *wireless* seperti hotspot komersial, ISP, Warnet, kampus-kampus maupun perkantoran sudah mulai memanfaatkan *wifi* pada jaringan masing - masing, tetapi sangat sedikit yang memperhatikan keamanan komunikasi data pada jaringan *wireless* tersebut. Hal ini membuat para hacker menjadi tertarik untuk mengexplore keamampuannya untuk melakukan berbagai aktifitas yang biasanya ilegal menggunakan jaringan *wireless*. Penyerangan yang dilakukan oleh *hacker* sangat bervariasi, mulai dari *Sniffing packet*, *packet injection*, *illegal authentication*, sampai *cracking* WEP, WPA/WPA2.

Keamanan jaringan *wireless* sangat dibutuhkan karena memiliki permasalahan yang lebih kritis dibandingkan jaringan kabel, dimana media udara yang digunakan dalam jaringan *wireless* tidak bisa dikontrol secara fisik.

Oleh karena itu, dibutuhkan dilakukannya audit keamanan terhadap jaringan *wireless* untuk mengetahui adanya potensi lubang keamanan (*security hole).* Sehingga diharapkan para administrator dan pengguna dapat meningkatkan metode keamanan dari celah-celah keamanan yang ditemukan, demi peningkatan kualitas keamanan dan produktivitas dari jaringan *wireless* tersebut. Point point keamanan yang ada jaringan *wireless* yang digunakan adalah dengan standar ISO 27001.

Instansi-instansi seperti BPKB DIKPORA Provinsi DIY merupakan salah satu contoh instansi yang menerapkan infrastruktur jaringan nirkabel. Sebagai instansi pemerintah, BPKB DIKPORA Provinsi DIY dituntut untuk meningkatkan pelayanan dilingkungan instansi terutama dibidang IT dengan penerapan jaringan *wireless* tersebut, maka harus mempersiapkan dan terus menganalisa keamanan jaringan *wireless* yang baik demi kinerja yang lebih handal. Oleh karena itu, karena pentingnya keamanan bagi instansi khususnya instansi pemerintahan, maka hal ini bertujuan mengetahui secara langsung secara aplikatif proses dan melakukan audit keamanan serta analisa kemungkinan-kemungkinan untuk melakukan

perbaikan dan peningkatan terhadap jaringan *wireless* di lingkungan tersebut.

1.2 Rumusan masalah

Berdasarkan latar belakang di atas dapat dirumuskan permasalahan yang akan di selesaikan dalam penelitian ini adalah:

1. Bagaimana mengidentifikasi lubang keamanan (*Security Hole*) di dalam jaringan WLAN (*Wireless Local Area Network*) BPKB DIKPORA Provinsi DIY?
2. Bagaimana melakukan pembuktian terhadap konsep *Wireless Hacking*?
3. Bagaimana melakukan *penetration test* terhadap keamanan jaringan WLAN BPKB DIKPORA Provinsi DIY ?
4. Bagaimana mencari solusi dan rekomendasi untuk meningkatkan keamanan jaringan WLAN berdasarkan audit keamanan jaringan *wireless* di BPKB DIKPORA DIY?

1.3 Batasan Masalah

Adapun batasan masalah dalam penelitian ini adalah sebagai berikut:

1. Melakukan audit terhadap keamanan jaringan *wireless* WLAN (*Wireless Local Area Network*) studi kasus di BPKB DIKPORA DIY.
2. Audit keamanan jaringan *wireless* dilakukan menggunakan standar ISO 27001
3. Melakukan audit menggunakan metodologi penetration test terhadap point-point keamanan jaringan *wireless* standar ISO 27001
4. Tidak membahas management jaringan, seperti konfigurasi server, dan management IP baik *privat* ataupun *publik*

1.4 Tujuan Penelitian

Adapun tujuan yang ingin dicapai dari penelitian ini adalah:

1. Menganalisis keamanan jaringan WLAN di BPKB DIKPORA Provinsi DIY
2. Melakukan audit terhadap keamanan jaringan WLAN di BPKB DIKPORA Provinsi DIY.
3. Membuat simulasi *penetration test* dengan melakukan skenario penyerangan untuk menguji kehandalan system keamanan yang di implementasikan dalam teknologi *wireless.*
4. Mencari solusi dan membuat rekomendasi untuk meningkatkan keamanan jaringan *wireless* berdasarkan hasil audit.

1.5 Manfaat Penelitian

Dengan adanya penelitian ini diharapkan banyak member manfaat, diantaranya:

1. Memberikan pemahaman mengenai konsep keamanan jaringan WLAN.
2. Memberikan gambaran mengenai mekanisme *wireless hacking*
3. Membantu *user* dan *administrator* jaringan WLAN di BPKB DIKPORA DIY dalam meningkatkan keamanan jaringan *wireless* yang digunakan.

1.6 Keaslian Penelitian

Adapun penelitian yang membahas tentang Audit keamanan jaringan *wireless* dengan menggunakan metodologi *wireless* security checklist standar ISO 27001 studi kasus di BPKB DIKPORA provinsi DIY setahu peneliti belum pernah dilakukan.

BAB 5

PENUTUP

5.1 KESIMPULAN

Berdasarkan pembahasan pada bab sebelumnya mengenai audit keamanan jaringan *wireless* pada BPKB DIKPORA DIY, maka kesimpulan yang dapat diambil diantaranya:

1. Infrastruktur jaringan *wireless* di BPKB DIKPORA DIY menggunakan 2 buah ISP (*Internet Service Provider*) yaitu JARDIKNAS dan JMN (Jogja Media Net) sehingga para pengguna jaringan *wireless* dapat menikmati layanan internet yang lebih cepat dan lebih stabil.

2. Dari Hasil Audit Keamanan *Wireless* didapati bahwa di instansi BPKB DIKPORA DIY belum memenuhi standar ISO 27001 tentang *Wireless Security* karena masih banyak point – point keamanan yang tertera pada *Wireless Security* ISO 27001 belum di inplementasikan pada instansi tersebut dan hanya memenuhi 21 point dari 56 point yang ada atau baru memenuhi 39,3 % dari keseluruhan point yang ada.

3. Dari hasil *Penetrationt test* didapati bahwa jaringan *Wireless* BPKB DIKPORA DIY menggunakan metode autentikasi WPA. metode autentikasi WPA di jaringan *Wireless* BPKB DIKPORA DIY masih bisa di tembus celah keamanannya.

4. Keamanan jaringan *wireless* yang berperan penting seperti, otentikasi koneksi jaringan *wireless* (seperti WEP, WPA, WPA2), kebijakan keamanan (*security policy*) sebagai aturan dasar (*basic rule*) untuk kelangsungan produktifitas jaringan *wireless*, dan *(Access Control List)* ACL sebagai manajemen *user* belum sepenuhnya diimplementasikan. Dan masih banyak standar keamanan jaringan *wireless* yang lainnya yang belum diimplementasikan, sehingga membuat jaringan *wireless* BPKB DIKPORA DIY masih sangat rentan terhadap upaya-upaya penyalahgunaan seperti penyusupan, penyerangan, pencurian *bandwith*, dan penyalahgunaan fasilitas jaringan *wireless* untuk keperluan pribadi. Hal-hal tersebut dikhawatirkan justru akan menjadi faktor desktruktif bagi produktifitas BPKB DIKPORA DIY.

5.2 SARAN

Dari hasil pengumpulan informasi dan pengalaman yang didapatkan saat melakukan Penelitian ini, ada beberapa saran yang dapat disampaikan untuk meningkatkan keamanan jaringan *wireless* :

1. Membuat dan mengimplementasikan kebijakan keamanan (*security policy*) agar tujuan dari keamanan jaringan *wireless* organisasi terarah dan terencana dengan baik, hal ini dibuat untuk memastikan kelangsungan produktifitas dari jaringan *wireless* sesuai dengan yang diharapkan.

2. Melakukan kontrol dan *maintenance* terhadap semua peralatan jaringan *wireless*, untuk memastikan semua peralatan jaringan *wireless* berada dalam area yang aman dan dalam kondisi yang baik. Di dalamnya termasuk

mengatur penempatan peralatan jaringan *wireless*, melakukan management signal *wireless*, melakukan *update firmware* secara teratur, melakukan management *bandwith*, dan melakukan *monitoring traffic* secara *real-time*. Hal tersebut berguna untuk mengantisipasi penyerangan DoS *(Denial of Service)* menggunakan metode RF jamming, dan akses langsung secara fisik oleh pihak yang tidak bertanggungjawab.

3. Membuat dan mengimplementasikan ACL *(Access Control List)*, untuk menentukan pihak-pihak yang diizinkan *(White List)* atau tidak diizinkan *(Black List)* untuk terhubung ke jaringan *wireless*. Salah satu implementasi dari ACL adalah menggunakan mekanisme *MAC Filtering*.

4. Mengaktifkan semua fitur keamanan jaringan *wireless* yang ada di WAP *(Wireless Access Point)*, yaitu mengaktifkan otentikasi koneksi menggunakan WPA2 dengan *passphare* yang tidak ada dalam kamus (untuk mengantisipasi *dictionary attack*) dan diganti secara berkala, kemudian mengaktifkan MAC *Filtering* yang merupakan implementasi dari ACL, mengganti *password default* dari area *administrator* WAP dan diganti secara berkala, mengganti IP *address* dan SSID *default* dari WAP, menon-aktifkan fitur broadcast SSID, serta mengaktifkan dan melakukan peninjauan secara berkala terhadap fitur *logging* yang ada di WAP.

5. Melakukan training atau penyuluhan mengenai resiko dan dampak dari penggunaan jaringan *wireless*, khususnya resiko dan dampak dibidang keamanan kepada pengguna jaringan *wireless*.

DAFTAR PUSTAKA

Christiantoro, Eddy. 2009. *Kajian Konsep Keamanan Pada Wireless Local Area Network*. Sekolah Teknik Elektro dan Informatika Institute Teknologi Bandung.

Febriyanto, Redya. 2008. *Pembangunan aplikasi pendeteksian serangan Deauthentication Frame dan ARP-requset replay pada jaringan IEEE 802.11 studi kasus : Aircrack-ng*. Sekolah Teknik Elektro dan Informatika Institute Teknologi Bandung.

http://www.smashingpasswords.com/files/wireless-lan-security-checklist.pdf Diakses pada 20 Desember 2010. Pukul 11.23

Geier, Jim. 2005. *Wireless Networks First-Step*. Yogyakarta: Penerbit ANDI

Odom, Wendell. 2004. *Computer Network First-Step*. Yogyakarta: Penerbit ANDI

Satya Ardhi Wardana, Hendrawan . 2005**.** *Analisa Proses Otentikasi dan Manajemen Kunci Pada WPA-PSK (Wi-fi Protected Acccess-Pre Shared Key) Terhadap Peningkatan Keamanan Komunikasi WLAN*. Departemen Teknik Elektro Institute Teknologi Bandung.

Stalling, William. 2004. *Network Security Essential*. Prentice Hall

Sukmaji, Anjik. 2008. *Jaringan Komputer***.** Yogyakarta: Penerbit ANDI

S'to. 2007. *Wireless Kungfu : Networking & Hacking*. Jakarta: Jasakom

Weber, Ron. 2000**.** *Information System control and Audit***.** Prentice Hall

Yani, Ahmad. 2008**.** *Panduan Membangun jaringan Komputer***.** Jakarta: Penerbit PT Kawan Pustaka

Yani, Ahmad. 2008**.** *Panduan Menjadi Teknisi jaringan Komputer***.** Jakarta: Penerbit PT Kawan Pustaka