Kajian Keamanan Jaringan *Wireless Local Area Network*
(*Proof of Concept* : *Wireless Hacking*)

SKRIPSI

Diajukan Kepada Fakultas Sains dan Teknologi

Universitas Islam Negeri Sunan Kalijaga

Untuk Memenuhi Sebagian Syarat Memperoleh Gelar Sarjana

Strata Satu Teknik Informatika

Disusun Oleh :

UKI SYUKRI GOZALI
NIM.06650047

PROGRAM STUDI TEKNIK INFORMATIKA

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.01.1/684/2011

Skripsi/Tugas Akhir dengan judul	:	Kajian Keamanan Jaringan Wireless Local Area Network (Proof of Concept : Wireless Hacking)
Yang dipersiapkan dan disusun oleh	:	
Nama	:	Uki Syukri Gozali
NIM	:	06650047
Telah dimunaqasyahkan pada	:	29 Maret 2011
Nilai Munaqasyah	:	A -

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

TIM MUNAQASYAH :

Ketua Sidang

Imam Riyadi, M.Kom
NIP. 60020397

Penguji I

Sumarsono, M. Kom
NIP.19710209 200501 1 003

Penguji II

M. Mustaqim, MT
NIP. 19790331 200501 1 004

Yogyakarta, 11 April 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 :
Lamp :

Kepada
Yth. Dekan Fakultas Sains dan 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 : Uki Syukri Gozali
NIM : 06650047
Judul Skripsi : Kajian Keamanan Wireless Local Area Network (Proof of concept : wireless hacking)

sudah dapat diajukan kembali kepada Program Studi Teknik Informatika Fakultas Sains dan Teknologi UIN *Sunan Kalijaga Yogyakarta* sebagai salah satu syarat untuk memperoleh gelar Sarjana Strata Satu dalam Program Studi Teknik Informatika

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

Yogyakarta, 28 Februari 2010
Pembimbing I

Imam Riadi, M.Kom
NIP. 50020397

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

SURAT PERSETUJUAN SKRIPSI/TUGAS AKHIR

Hal :
Lamp :

Kepada
Yth. Dekan Fakultas Sains dan 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	: Uki Syukri Gozali
NIM	: 06650047
Judul Skripsi	: Kajian Keamanan Wireless Local Area Network (Proof of concept : wireless hacking)

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

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

Yogyakarta, 28 Februari 2010
Pembimbing II

Bambang Sugiantoro, MT
NIP. 19751024 2009 12 1 002

PERNYATAAN KEASLIAN SKRIPSI

Yang bertanda tangan di bawah ini :

Nama	: Uki Syukri Gozali
NIM	: 06650047
Program Studi	: Teknik Informatika
Fakultas	: Sains dan Teknologi

Dengan ini saya menyatakan bahwa skripsi saya yang berjudul **"Kajian Keamanan *Wireless Local Area Network* (*Proof of Concept* : *Wireless Hacking*)"** adalah benar-benar karya saya sendiri. Sepanjang sepengetahuan saya tidak terdapat karya atau pendapat yang ditulis atau diterbitkan orang lain kecuali sebagai acuan atau kutipan dengan mengikuti tata penulisan ilmiah yang lazim dan disebutkan dalam daftar pustaka.

Yogyakarta, 28 Februari 2011

Yang menyatakan,

METERAI TEMPEL 325A4AAF403888613 6000 DJP

Uki Syukri Gozali

NIM. 06650047

MOTTO

Kebanyakan milyuner mendapat nilai B atau C di kampus. Mereka membangun kekayaan bukan dari IQ semata, melainkan kreativitas dan akal sehat

"Most millionaires got a B or C on campus. They build wealth rather than IQ alone, but creativity and common sense"

~Thomas Stanley~

Saya memang bodoh di suatu bidang,tapi inovasi dan kreatifitas membuat saya lebih ahli di bidang yang lain. . . "out of the box".

I was stupid in a field, but innovation and creativity makes me more experts in other fields. . . "out of the box ".

~Uki Syukri Gozali~

مَنْ سَلَكَ طَرِيقًا يَلْتَمِسُ فِيهِ عِلْمًا سَهَّلَ اللَّهُ لَهُ طَرِيقًا إِلَى الْجَنَّةِ

Barangsiapa berjalan di suatu jalan untuk mencari ilmu, niscaya Allah akan memudahkan baginya jalan ke surga.

~Al-Hadits~

PERSEMBAHAN

Skripsi ini aku persembahkan :

untuk kemajuan Islam dan negara tercinta Indonesia.

Skripsi ini aku dedikasikan :

untuk almamater tercinta Program Studi Teknik Informatika Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta.

Skripsi ini aku dedikasikan :

untuk kedua orang tua ku, semoga bisa sedikit membasuh peluh, air mata, dan darah mereka dalam mendidik dan membesarkanku.

KATA PENGANTAR

Puji syukur selalu dipanjatkan kehadirat Allah SWT karena dengan rahmat dan karunia-Nyalah maka penulis telah berhasil menyelesaikan penulisan skripsi dengan judul ”Kajian Keamanan Jaringan *Wireless Local Area Network (Proof of Concept : Wireless Hacking)*”. Sholawat serta salam penulis tunjukkan kepada junjungan umat Nabi Muhammad SAW.

Penyelesaian penulisan skripsi ini tidak terlepas dari dukungan banyak pihak yang telah banyak memberikan arahan, bantuan pemikiran, doa, semangat dan lain sebagainya. Oleh karena itu, pada kesempatan ini penulis menyampaikan rasa terima kasih kepada:

1. Bapak Prof. Drs. H. Akh. Minhaji, M.A, Ph.D selaku Dekan Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta.
2. Bapak Agus Mulyanto, M.Kom selaku Ketua Program Studi Teknik Informatika Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga Yogyakarta.
3. Bapak Imam Riadi, M.Kom dan Bapak Bambang Sugiantoro MT,CompTIA selaku dosen pembimbing skripsi yang telah banyak membimbing penulis sehingga laporan ini dapat berjalan dengan lancar.
4. Bapak Drs.St. Mulyanta M.Kom selaku pembimbing lapangan di BPKB DIKPORA Provinsi DIY.

5. Dosen Program Studi Teknik Informatika yang banyak memberikan masukan ilmu kepada penulis.
6. Ayahanda H. Mas'ud, M.pd dan Ibunda Nur Aisyah yang dengan kasih sayang dan cinta kasih yang tulus diberikan kepada penulis sehingga dapat memberikan motivasi semangat untuk terus berkarya demi terwujudnya cita-cita yang mulia.
7. Saudara-saudaraku yang tercinta Nunik Rifa'atul Mahmudah dan Burhanudin Yusuf terima kasih atas semangat dan do'a yang tulus.
8. Teman-teman seperjuangan di UIN Sunan Kalijaga terima kasih atas dukungan dan kebaikannya.
9. Semua pihak yang tidak dapat penulis sebutkan satu persatu yang telah memberikan dukungan dan semangat sehingga penulis dapat menyelesaikan penulisan skripsi ini.

Semoga skripsi ini dapat bermanfaat bagi semua dan semoga amal baik yang telah diberikan dapat diterima di sisi Allah Swt, amin.

Yogyakarta, 1 Maret 2011

Penulis

<u>UKI SYUKRI GOZALI</u>

NIM : 06650047

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

Kajian Keamanan Jaringan *Wireless Local Area Network*

(*Proof of Concept* : *Wireless Hacking*)

Oleh :

Uki Syukri Gozali
NIM.06650047

ABSTRAK

Medium udara yang sulit dikontrol dalam jaringan *wireless*, membuat jaringan *wireless* rentan terhadap potensi penyerangan dan penyusupan. Penelitian ini diharapkan dapat memberikan kontribusi bagi peningkatan keamanan jaringan *wireless*, khususnya jaringan WLAN (*Wireless Local Area Network*).

Penelitian ini mengkaji metode penyerangan dalam jaringan *wireless* (*wireless hacking*) yang dilakukan oleh penyerang atau penyusup dengan melakukan uji penetrasi (*penetration testing*) terhadap metode-metode pengamanan jaringan WLAN. Uji penetrasi meliputi *reveal SSID* (*Service Set Identifier*), *MAC address spoofing*, *cracking WEP* (*Wired Equivalent Privacy*), *cracking WPA/WPA2-PSK* (*Wifi Protected Access-Pre Shared Key*).

Berdasarkan hasil pengujian dapat diketahui metode-metode yang dilakukan oleh penyerang atau penyusup untuk mendapatkan akses ke jaringan *wireless*, sehingga dapat dilakukan berbagai langkah antisipasi untuk mengurangi resiko penyerangan dan penyusupan tersebut.

Kata Kunci : *Wireless Local Area Network*, WEP, WPA, *Hacking*, SSID

STUDI OF SECURITY IN WIRELESS LOCAL AREA NETWORK

(Proof of Concept : Wireless Hacking)

Uki Syukri Gozali
NIM.06650047

ABSTRACT

Air medium are difficult to control in wireless networks, creating a wireless network vulnerable to potential attacks and intrusions. This research is expected to contribute to the increase in wireless network security, especially WLAN (Wireless Local Area Network).

This study examines methods of attack in wireless networks (wireless hacking) conducted by the attacker or intruder to perform penetration testing (penetration testing) against the methods of securing WLAN networks. Penetration test covers reveal the SSID (Service Set Identifier), MAC address spoofing, cracking WEP (Wired Equivalent Privacy), cracking WPA/WPA2-PSK (Wifi Protected Access-Pre Shared Key).

Based on the results of this test, it is known the methods performed by the attacker or intruder to gain access to wireless network, so it can be done various anticipatory measures to reduce the risk of attack and intrusion.

Keywords : Wireless Local Area Network, WEP, WPA, Hacking, SSID

BAB 1

PENDAHULUAN

1.1 Latar Belakang Masalah

Teknologi *wireless* menawarkan beragam kemudahan, kebebasan dan fleksibilitas yang tinggi. Teknologi *wireless* memiliki cukup banyak kelebihan dibandingkan teknologi kabel yang sudah ada. Kita bisa menikmati kemudahan akses komunikasi data dan akses *internet* di posisi mana pun selama masih berada dalam jangkauan *wireless*.

Selain menawarkan berbagai kemudahan dalam jaringan *wireless* atau WLAN (*Wireless Local Area Network*), terdapat resiko keamanan yang lebih kritis dibandingkan dengan jaringan kabel karena medium udara dalam jaringan *wireless* tidak bisa dikontrol secara fisik. Hal ini membuat para penyerang atau penyusup (hacker) menjadi tertarik untuk melakukan berbagai aktifitas yang biasanya ilegal terhadap jaringan *wireless* (WLAN). Penyerangan yang dilakukan oleh *hacker* sangat bervariasi, mulai dari *Sniffing packet*, *packet injection*, *illegal authentication*, sampai *cracking* WEP (*Wired Equivalent Privacy*), dan *cracking* WPA (*Wifi Protected Access*) / WPA2.

Oleh karena itu, dibutuhkan dilakukannya kajian terhadap konsep keamanan jaringan WLAN (*Wireless Local Area Network*) untuk mengetahui metode-metode yang dilakukan oleh para *hacker* dalam melakukan penyerangan, dengan melakukan pembuktian terhadap ancaman dan serangan dalam jaringan

wireless. Sehingga diharapkan dapat mencari solusi bagi para pengguna (*user*) maupun *administrator* untuk meningkatkan metode keamanan jaringan *wireless* dari celah-celah keamanan yang ditemukan, demi peningkatan kualitas keamanan dan produktivitas dari jaringan *wireless* tersebut.

1.2 Rumusan Masalah

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

1. Bagaimana mengidentifikasi lubang keamanan (*security hole*) di dalam jaringan WLAN (*wireless local area network*)?
2. Bagaimana melakukan metode *Proof of Concept* terhadap *wireless hacking*?
3. Bagaimana mencari solusi untuk meningkatkan keamanan jaringan WLAN berdasarkan hasil dari pembuktian konsep *wireless hacking*?

1.3 Batasan Masalah

Adapun batasan masalah dalam penelitian ini adalah sebagai berikut :

1. Melakukan kajian konsep keamanan jaringan *wireless* berbasis protokol IEEE 802.11 (WLAN).
2. Kajian keamanan jaringan *wireless* dilakukan menggunakan metode *Proof of Concept* dari *wireless hacking*.
3. Kajian keamanan jaringan wireless dilakukan di Laboratorium Pusat Komputer (Puskom) BPKB DIKPORA Provinsi DIY.

4. Melakukan *wireless hacking* menggunakan *penetration test* terhadap protokol keamanan jaringan *wireless* IEEE 802.11 (WLAN) dan *penetration test* dilakukan menggunakan metode *black-box hacking*.
5. Melakukan mekanisme *wireless hacking*, seperti *Reveal* SSID, MAC *Spoofing*, *Cracking* WEP, *Cracking* WPA/WPA2 PSK (*Pre Shared Key*).

1.4 Tujuan Penelitian

Adapun tujuan yang ingin dicapai dari penelitian ini adalah :

1. Menganalisa cara kerja metode keamanan jaringan WLAN.
2. Melakukan pembuktian terhadap konsep *wireless hacking*.
3. Membuat simulasi *penetration test* dengan melakukan skenario penyerangan untuk menguji kehandalan sistem keamanan yang diimplementasikan dalam teknologi *wireless*.
4. Mencari solusi dan membuat rekomendasi untuk meningkatkan keamanan jaringan *wireless* berdasarkan hasil pembuktian konsep *wireless hacking*.

1.5 Manfaat Penelitian

Dengan adanya penelitian ini diharapkan banyak memberikan manfaat, diantaranya:

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

1.6 Keaslian Penelitian

Adapun penelitian yang berhubungan dengan Kajian Keamanan Jaringan *Wireless Local Area Network* sudah pernah dilakukan sebelumnya, yaitu Kajian Konsep Keamanan Pada *Wireless Local Area Network* (Eddy Christian, 2009), penelitian tersebut melakukan kajian terhadap keamanan standar dari jaringan *wireless*, dengan membangun *environment* jaringan wireless menggunakan beberapa *soekris*, kemudian melakukan pengujian terhadap *environment* jaringan *wireless* tersebut, adapun pengujian yang dilakukan berupa *Cracking WEP, Cracking WPA, Url Sniff, Denial of Service, DNS Spoofing, Sniffing Password, dan Sidejacking*. Pengujian tersebut lebih memfokuskan jaringan *wireless* sebagai media *hacking*. Sedangkan penelitian yang dilakukan disini menitik beratkan pada Kajian Keamanan *Wireless Local Area Network* (*Proof of Concept* : *Wireless Hacking*) yang memfokuskan penelitian pada pembuktian konsep dari *wireless hacking*, dimana *environment* yang dibangun menggunakan *access point* dan pengujian yang dilakukan memfokuskan pada standar keamanan jaringan IEEE 802.11 (WLAN) sebagai objek pengujian, dan mengkaji metode yang digunakan oleh *hacker* untuk melakukan *gaining access* terhadap jaringan *wireless* tersebut, dan penelitian tersebut setahu peneliti belum pernah dilakukan.

BAB V

KESIMPULAN

5.1 Kesimpulan

Berdasarkan hasil pengujian terhadap kelemahan jaringan *wireless local area network* (WLAN), didapatkan kesimpulan sebagai berikut :

1. Identifikasi lubang keamanan dilakukan menggunakan metode *scanning wireless* dan *penetration test*.

3. Penggunaan *hidden SSID*, *MAC Filtering*, dan WEP sebagai metode pengamanan WLAN bukan merupakan pilihan yang efektif.

4. Untuk pemakaian personal maupun jaringan *wireless* berskala menengah kebawah, WPA/WPA2 PSK merupakan pilihan yang masih bisa diandalkan dengan syarat penggunaan *passphare*/ *secret key* yang unik dan dilakukan pergantian *passphare*/ *secret key* secara periodik.

5. *Captive portal* merupakan solusi alternatif dalam mengamankan jaringan *wireless*, integrasi *router* dan *firewall* dalam *captive portal* menjadi nilai tambah tersendiri bagi *administrator* dalam melakukan *monitoring*, manajemen dan tindakan pengamanan terhadap jaringan *wireless*.

5.2 Saran

Saran yang dapat diberikan oleh peneliti terkait dengan keamanan jaringan WLAN (*wireless local area network*) adalah sebagai berikut :

1. Menggunakan kombinasi berbagai metode pengamanan jaringan WLAN.
2. Memperketat kebijakan keamanan (*security policy*) khususnya kontrol akses terhadap penggunaan sumber daya WLAN.
3. Melakukan audit keamanan secara rutin terhadap jaringan WLAN, audit tersebut dapat dilakukan oleh internal auditor maupun eksternal auditor.
4. Melakukan *update firmware* maupun *patching* secara rutin terhadap perangkat jaringan WLAN.
5. Mengevaluasi dan meningkatkan kemampuan *administrator* di bidang keamanan jaringan.

DAFTAR PUSTAKA

Aircrack-ng, 2007. ***Aircrack-ng Documentation***. http://www.aircrack-ng.org akses 27 oktober 2010

Arifin, Zainal. 2008. ***Sistem Pengamanan Jaringan Wireless LAN Berbasis Protokol 802.1x dan Sertifikat***. Yogyakarta : Penerbit ANDI

Christian, 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.

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

NIST. 2008. ***Guide to Securing Legacy IEEE 802.11 Wireless Network***. U.S. Department of Commerce

Pentakalos, Odysseas. 2008. ***Proof of Concept Design***. http://msdn.microsoft.com/en-us/library/cc168618.aspx akses 27 oktober 2010

Roman, Mihail dkk. 2005. ***Reverse Engineering of Aircrack Software***. Concordia University. http://laurent.fallet.free.fr akses 27 Oktober 2010

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.

Stamp, Mark dan Low M Richard. 2007. ***Applied Cryptanalysis : Breaking Chiper in The Real World***. Wiley Interscience

Sinambela, Joshua M. 2007. ***Seminar Open Source dan Wireless Hacking***. Yogyakarta : AMIKOM.

Sofwana, Iwan. 2010. ***CISCO CCNA & Jaringan Komputer***. Bandung: Penerbit INFORMATIKA

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

Tews, Erik. 2005. ***Attacks on WEP Protocol***. http://aircrack-ng.org akses 27 Oktober 2010