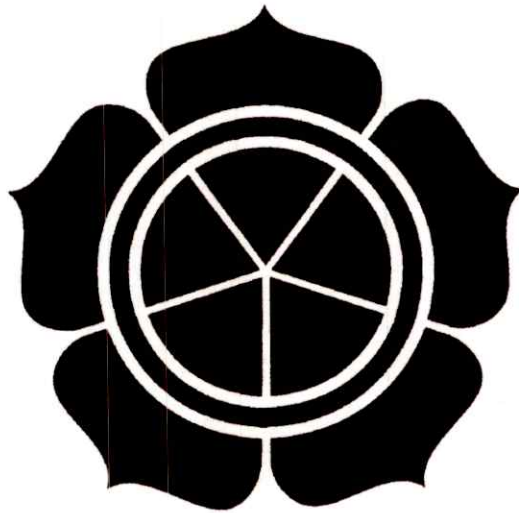


**STUDI KASUS CELAH KEAMANAN PADA JARINGAN NIRKABEL
YANG MENERAPKAN WEP (*WIRED EQUIVALENT PRIVACY*)**

SKRIPSI



oleh :

M. Agung Nugroho (03.11.0199)

**TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
STMIK AMIKOM YOGYAKARTA
YOGYAKARTA
2007**

HALAMAN PENGESAHAN

STUDI KASUS CELAH KEAMANAN PADA JARINGAN NIRKABEL YANG MENERAPKAN WEP (*WIRED EQUIVALENT PRIVACY*)

Skripsi

Disusun sebagai persyaratan untuk memperoleh gelar Sarjana Komputer

**Jurusan Teknik Informatika
Sekolah Tinggi Manajemen Informatika dan Komputer
AMIKOM Yogyakarta**

Disetujui dan disahkan oleh :

Ketua STMIK AMIKOM Yogyakarta

Dosen Pembimbing



(Drs. M. Suyanto, MM)



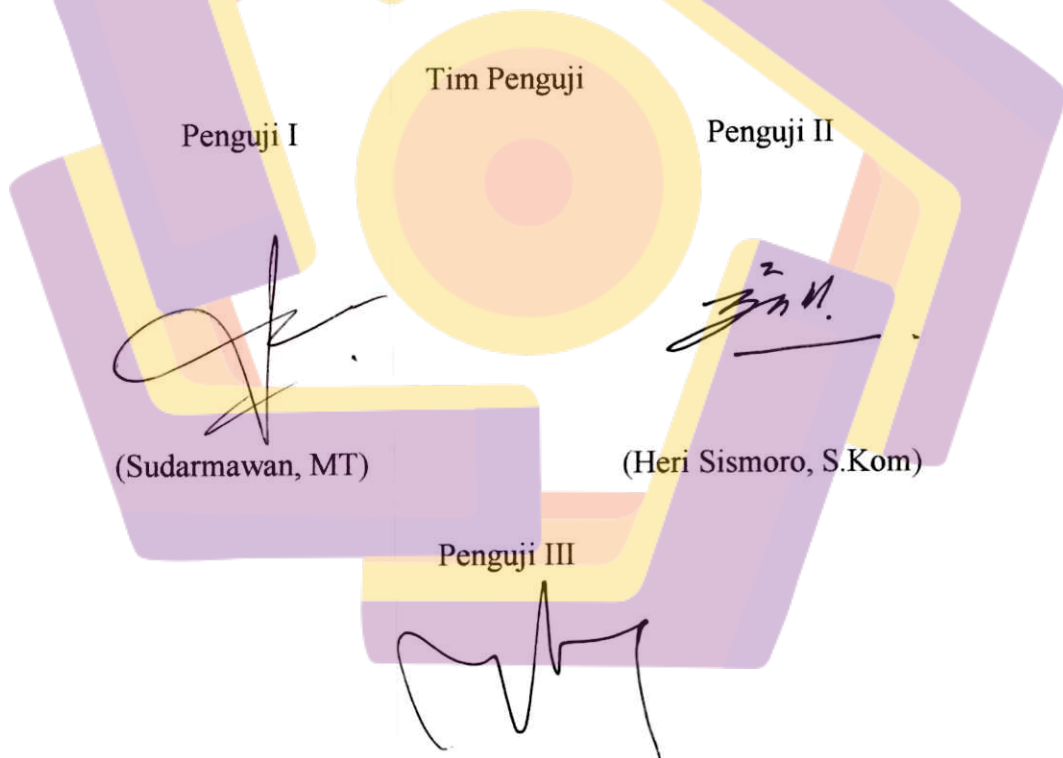
(Sudarmawan, MT)

HALAMAN BERITA ACARA

STUDI KASUS CELAH KEAMANAN PADA JARINGAN NIRKABEL YANG MENERAPKAN WEP (*WIRED EQUIVALENT PRIVACY*)

Laporan ini telah dipertahankan dan diajukan oleh **M.Agung Nugroho** didepan Tim Penguji Jurusan Teknik Informatika sebagai syarat kelulusan Srata 1 Teknik Informatika STMIK AMIKOM Yogyakarta, pada:

Hari : Senin
Tanggal : 28 Mei 2007
Jam : 12.30 WIB
Tempat : Ruang Network



(Ir. Rum Muhammad Andre KR, M.Kom)

HALAMAN PERSEMBAHAN

Skripsi ini penulis persembahkan untuk :

- Allah Subhana wata 'ala yang telah memberikan Karunia, Rahmat serta kesehatan dan kesempatan kepada penulis, sehingga dapat terselesaikan skripsi ini.
- Ayah dan ibu yang selalu memberikan dukungan mental, moril dan doa yang selalu menyertai penulis, serta kakakku Fajar dan adikku Dian yang selalu ceria dan menghibur penulis.
- Dosen pembimbingku yang selalu sabar dan teliti bapak Sudarmawan, ST.
- Mas Josua Sinambela yang telah meminjamkan AP dan memberikan masukan-masukan untuk skripsi ini, BTW sorry udah ngerusakin usb wireless prismnya :((.
- Sahabatku Edo, Sari, Hasna, Deni, AJ dan Budi yang selalu memberikan nasehat dan semangat sekaligus tempat curhat serta mbak nila yang udah mau jadi kakak sekaligus tempat curhat selama ini.
- Seluruh Teman-teman ; -Linuxer- Manda, Hari, Zaq, Awal, Wardi, Rido, Dion, Enggar, stwn, mas Fathir, mas Aar, Okto , mas fathur, piko, lilik dan smua yang merasa sbg linuxer ; -blogger- Zam, Leo, Ai, Thestoopid, Devishanty, Tikabanget dan seluruh teman bloggerQ ; -OS- Farhan, Yoga, Deni, Ingram, Fitri, Sasuke, Gero, amel, Vera dan seluruh Onegai Anbu ; -another- Ira Feby, Ira GT, Noprie, Meika, Mega, Ria, Kiky, Ayu, Deny, Indra, Diwang, Adit, Irfan, Aji dan semua teman-temanQ yang tidak dapat kusebutkan satu persatu (Thanx banget buat support dan doanya).
- Terakhir untuk teman sekaligus dosen pak Hanafi, pak Melwins, pak Suwanto, mas Rico.

KATA PENGANTAR

Assalamu'alaikum warahmatullahi wabarakatuh

Dengan menyebut nama Allah Subhana wata 'ala yang maha pengasih dan penyayang, puji syukur kehadiran Allah Subhana wata 'ala yang telah melimpahkan rahmat, taufiq dan hidayahnya kepada hambanya. Semoga sholawat dan salam selalu dilimpahkan kepada Nabi Muhammad Sholalhu 'Alaihi Wassalam, keluarganya, sahabat dan pengikut beliau yang beriman sampai hari akhir.

Skripsi yang berjudul “Studi Kasus Celah Keamanan Jaringan Nirkabel yang Menerapkan WEP (Wired Equivalent Privacy) semoga dapat bermanfaat bagi siapapun dan bagi yang mengembangkan lebih lanjut. Semoga dengan adanya penelitian ini dapat lebih bermanfaat bagi para administrator maupun pengguna jaringan nirkabel dalam menanggapi isu keamanan.

Semoga ilmu yang telah diperoleh dapat bermanfaat baik bagi penulis maupun bagi pembaca.

Wa 'alaikum salam warahmatullahi wabarakatuh

Jogjakarta, 25 mei 2007

M. Agung Nugroho

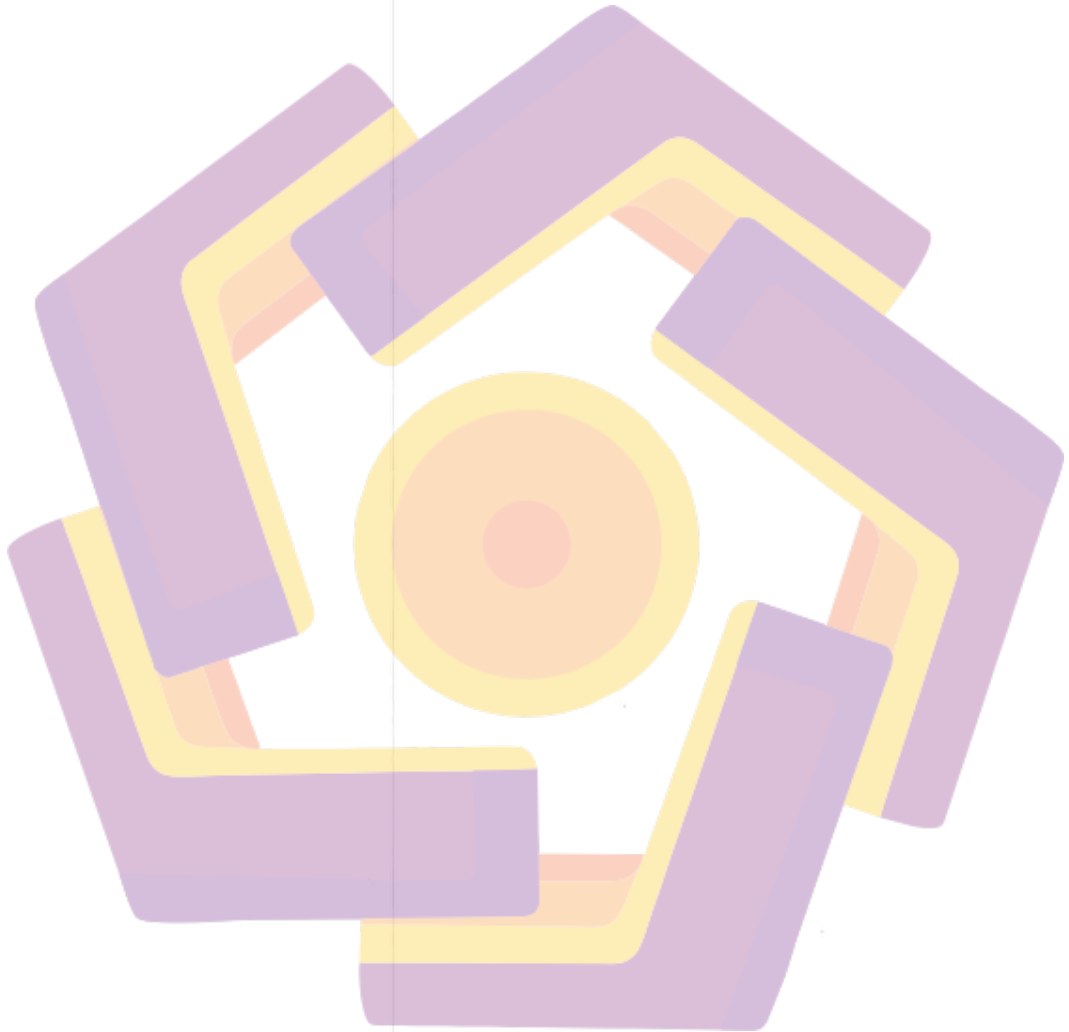
HALAMAN JUDUL.....	i
HALAMAN PENGESAHAN.....	ii
HALAMAN BERITA ACARA.....	iii
HALAMAN PERSEMBAHAN.....	iv
KATA PENGANTAR.....	v
DAFTAR ISI.....	vi
DAFTAR TABEL.....	xi
DAFTAR GAMBAR.....	xii
ABSTRAKSI.....	xiii
BAB I PENDAHULUAN.....	1
1.1 Latar belakang Masalah.....	1
1.2 Perumusan Masalah.....	3
1.3 Batasan Masalah.....	3
1.4 Maksud dan Tujuan.....	5
1.5 Metode Penelitian.....	6
1.6 Sistematika Penulisan.....	7
1.7 Jadwal Penelitian.....	8
BAB II LANDASAN TEORI.....	9
2.1 Tinjauan Pustaka	9
2.1.1 Manfaat Audit Jaringan Nirkabel yang Menerapkan WEP.....	11
2.2 Landasan Teori.....	11
2.2.1 Jaringan Nirkabel (Wireless LAN).....	11

2.2.2	Wi-Fi (Wireless Fidelity).....	12
2.2.3	Standart IEEE 802.11.....	12
2.2.4	Arsitektur Jaringan Nirkabel.....	14
2.2.4.1.	Independent Basis Service Set (IBSS).....	14
2.2.4.2.	Basis Service Set (BSS).....	14
2.2.4.3.	Extended Service Set (ESS).....	15
2.2.5	Wired Equivalent Privacy (WEP).....	16
2.2.5.1.	Initialization Vector (IV).....	17
2.2.5.2.	CRC 32.....	18
2.2.5.3.	Operasi WEP.....	18
2.2.5.4.	Kelemahan WEP.....	19
2.2.6	Fitur Keamanan Dasar Jaringan Nirkabel.....	20
2.2.6.1.	Service Set Identifier (SSID).....	20
2.2.6.2.	Wired Equivalent Privacy (WEP).....	20
2.2.6.3.	Filtering MAC Address.....	20
2.2.7	Penyerangan pada Jaringan Nirkabel.....	20
2.2.7.1.	Sniffing dan Eavesdrop.....	21
2.2.7.2.	Brute Force Attack.....	21
2.2.7.3.	Man-in-the-middle Attack.....	21
2.2.7.4.	Denial of Service Attack.....	21
2.2.7.4.	Packet Injection.....	21
BAB III CARA PENELITIAN.....		22

3.1. Objek Penelitian.....	22
3.2. Alat Penelitian.....	22
3.2.1. Infrastruktur Komputer.....	22
3.2.1.1. Komputer Penyerangan (Hacker).....	22
3.2.1.2. Komputer klien target.....	23
3.2.2. Infrastruktur Jaringan.....	23
3.2.3. Infrastruktur Perangkat Lunak.....	24
3.2.3.1. Sistem Operasi.....	24
3.2.3.2. Madwifi Driver.....	25
3.2.3.3. Wireless-tools.....	25
3.2.3.4. Kismet.....	25
3.2.3.5. Aircrack.....	26
3.2.3.6. Aircsnort.....	26
3.3. Langkah-langkah Penelitian.....	27
3.3.1. Access Point.....	27
3.3.2. Komputer Klien Target.....	30
3.3.3. Komputer Penyerang (Hacker).....	31
3.3.3.1. Madwifi Driver.....	31
3.3.3.2. Wireless-tools.....	31
3.3.3.3. Kismet.....	31
3.3.3.4. Aircrack.....	33
3.3.3.5. Aircsnort.....	33

3.4. Langkah-langkah Pengujian.....	35
3.4.1. Footprinting.....	37
3.4.1.1. Deteksi SSID.....	37
3.4.1.2. Pengumpulan Informasi Target.....	38
3.4.2. Sniffing Packet.....	39
3.4.3. Cracking WEP.....	41
3.4.4. Packet Injection.....	43
3.4.5. Masuk kedalam Jaringan Target.....	45
BAB IV HASIL PENGUJIAN DAN PEMBAHASAN	47
4.1. Footprinting.....	47
4.2. Pembuktian kelemahan WEP.....	48
4.2.1. Penyerangan Level Teori.....	48
4.2.2. Penyerangan dengan Metode FMS.....	51
4.2.3. Pengembangan Penyerangan Metode FMS.....	52
4.2.3.1. Sniffing Packet.....	53
4.2.3.1. Packet Injection.....	55
4.2.3.3. Cracking WEP.....	57
4.3. Solusi.....	59
4.3.1. Filtering MAC Address dan IP Address.....	59
4.3.2. Filtering ARP.....	61
4.3.3. Wireless Distribution System (WDS).....	62
4.3.3. Captive Portal.....	62

4.3.5. Menggunakan Metode Keamanan WPA dan 802.1x.....	63
BAB V KESIMPULAN DAN SARAN.....	64
5.1. Kesimpulan.....	64
5.2. Saran.....	65
DAFTAR PUSTAKA.....	67



DAFTAR TABEL

Tabel.1-1. Jadwal Penelitian.....	8
Tabel 2-1. Karakteristik dasar standart jaringan nirkabel.....	12
Tabel 3-1. Spesifikasi komputer penyerang (<i>hacker</i>).....	23
Tabel 3-1. Spesifikasi komputer klien target.....	23
Tabel.4-1. Chipertext “a”.....	48
Tabel.4-2. Chipertext “b”.....	49
Tabel.4-3. XOR Chipertext “a” dan “b”.....	49
Tabel.4-4. XOR Plaintext “a” dan “b”.....	49
Tabel.4-5.Percobaan penyerangan metode FMS pada WEP 64-bit.....	51
Tabel 4-6. Tabel keterangan Field pada tool airodump.....	53
Tabel 4-7. Pengaruh packet injection pada klien.....	55
Tabel.4-8.Percobaan penyerangan dengan mengembangkan metode FMS pada WEP 64-bit.....	57

DAFTAR GAMBAR

Gambar.2-5. Topologi IBSS atau ad-hoc.....	14
Gambar.2-6. Topologi BSS.....	15
Gambar.2-7. Topologi ESS.....	15
Gambar.2-1. Rangkaian urutan enkripsi WEP.....	16
Gambar.2-2. Enkripsi WEP.....	17
Gambar.2-3. Area yang dienkripsi dan tidak dienkripsi.....	19
Gambar.3-1. Topologi jaringan nirkabel dan skenario penyerangan.....	24
Gambar.3-2. Login ke AP.....	27
Gambar.3-3. Masuk ke dalam menu AP.....	28
Gambar.3-4. Konfigurasi AP.....	28
Gambar.3-5. Konfigurasi WEP pada AP.....	29
Gambar.3-6. Konfigurasi IP dan DHCP.....	29
Gambar.3-7. Proses WEP cracking jaringan nirkabel.....	35
Gambar.3-8. Kismet Interface.....	37
Gambar.3-9. Opsi sort pada kismet.....	38
Gambar.3-10. Informasi pada jaringan yang terpilih.....	49
Gambar.3-11. Sniffing packet.....	41
Gambar.3-12. Cracking WEP.....	43
Gambar.3-13. Packet injection dengan aireplay.....	44
Gambar.4-1. Hasil footprinting.....	47
Gambar 4-3. Hasil cracking dengan metode penyerangan FMS.....	51
Gambar 4-4. Hasil Sniffing dengan airodump.....	53
Gambar 4-5. Hasil packet injection menggunakan aireplay.....	55
Gambar 4-6. Format ARP Header yang mengandung IP dan MAC address.....	56
Gambar 4-7. Hasil cracking dengan mengembangkan metode FMS.....	57
Gambar 4-8. Filtering Mac Address pada AP.....	59



ABSTRAKSI

Dengan semakin berkembang dan populernya jaringan nirkabel, menyebabkan munculnya isu-isu keamanan pada jaringan nirkabel. Serangan terhadap jaringan nirkabel pun berkembang. Penyerangan yang dilakukan oleh *hacker* sangat bervariasi, mulai dari *wardriving (footprinting)*, *Sniffing packet*, *packet injection* sampai *cracking WEP*. Serangan ini juga yang penulis gunakan untuk melakukan audit.

Penulis melakukan audit terhadap jaringan nirkabel yang menerapkan WEP, dengan memanfaatkan tiga kelemahan, yaitu *keystream reuse*, berasal dari kesalahan manajemen IV ; Keterbatasan numerical 24-bit pada IV, yang menghasilkan nilai 16.777.216 ; Kelemahan pada protokol WEP yaitu tidak dapat memfilter replay paket yang dikirimkan.

Dari audit tersebut, penulis melakukan langkah antisipasi untuk mengurangi resiko penyerangan dengan menggunakan *access control* atau melakukan pembatasan terhadap MAC address dan IP address, *filtering ARP*, WDS (*Wireless Distribution System*), *Captive Portal*, dan diharapkan para administrator dan pengguna mulai meninggalkan metode keamanan WEP dan beralih menggunakan metode keamanan terkini seperti WPA dan 802.1x.