BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Jaringan nirkabel merupakan solusi untuk komunikasi yang tidak bisa dilakukan dengan jaringan yang menggunakan kabel. Misalnya orang yang ingin mendapatkan informasi atau melakukan komunikasi walaupun sedang berada didalam mobil atau pesawat terbang, maka mutlak jaringan nirkabel (*wireless network*) diperlukan karena koneksi kabel tidaklah mungkin dibuat didalam mobil ataupun pesawat. Saat ini jaringan nirkabel sudah marak digunakan dengan memanfaatkan jasa satelit dan mampu memberikan kecepatan akses yang lebih cepat dibandingkan dengan jaringan yang menggunakan kabel.

Dengan semakin berkembang dan populernya jaringan nirkabel, menyebabkan munculnya isu-isu keamanan pada jaringan nirkabel. Popularitas disebabkan oleh 2 faktor utama yaitu kemudahan dan biaya yang murah. Karena kemudahannya, vedor-vendor pun mulai menghasilkan produk-produk hardware dengan standart *Institute of Electrical and Electronics Engineer* (IEEE) 802.11 dan hardware tersebut dibandrol dengan harga yang wajar.

Walaupun demikian, kemudahan pada jaringan nirkabel (*wireless Local Area Network*) juga menyebabkan permasalahan keamanan baru yang tidak pernah ada pada jaringan kabel. Dengan koneksi ke jaringan tanpa menggunakan kabel, secara tidak langsung lalu lintas (*traffic*) data akan dilewatkan melalui udara dan memungkinkan setiap orang untuk mengambil data yang lewat (*Sniffing*) dan melakukan decoding pada data tersebut.

Berbagai penelitian WEP telah dilakukan dan diperoleh bahwa walaupun jaringan nirkabel terlindungi oleh WEP, pihak ketiga (*hacker*) tetap dapat membobol masuk [1]. Penelitian lain pada beberapa negara juga menunjukkan

1 Jim Geovedi, 2004.

bahwa penggunaan WEP hanya digunakan tidak lebih dari 25% pengguna [2]. Dari hasil penelitian tersebut, penulis tertarik melakukan *wardriving,* dan menemukan fakta bahwa sebagian besar *access point* (AP) memang tidak menerapkan WEP sebagai metode keamanan. Yang menjadi keluhan dari pengaktifan WEP adalah kecepatan koneksi menjadi berkurang secara drastis, ada yang mengatakan penurunan *throughput* dengan menggunakan WEP bisa sampai 1 MB untuk metode enkripsi 64-bit dan 2 MB untuk metode enkripsi 128-bit [3]. Sehingga banyak di antara mereka yang memilih untuk tidak menggunakan perlindungan enkripsi WEP.

Dari kelemahan tersebut, ternyata membawa beberapa peneliti dan *hacker* untuk melakukan analisa untuk membuktikan kelemahan WEP. Sehingga berkembanglah perangkat lunak bebas yang digunakan untuk menunjukkan kelemahan pada WEP seperti AirSnort, dan dapat melakukan *recovery* pada kunci yang terenkripsi.

Serangan terhadap jaringan nirkabel pun berkembang. Penyerangan yang dilakukan oleh *hacker* sangat bervariasi, mulai dari *wardriving* (*footprinting*), *Sniffing packet*, *ARP Spoofing* sampai pembobolan kunci enkripsi dengan proses *brute-force*. Serangan-serangan tersebut merupakan cara-cara yang dilakukan *hacker* untuk mendapatkan kunci enkripsi.

Karena banyaknya serangan yang dilakukan oleh pihak ketiga (*hacker*) dengan memanfaatkan celah keamanan tersebut, maka penulis tertarik untuk melakukan penelitian dengan analisa dan audit celah keamanan WEP dengan menggunakan cara kerja pihak ketiga (*hacker*) dalam melakukan praktek *hacking*, dalam kasus ini adalah *cracking* WEP. Dari cara kerja tersebut, penulis dapat mengambil langkah penanggulangan terhadap celah tersebut.

Untuk alasan tersebut penulis memilih judul "STUDI KASUS CELAH KEAMANAN PADA JARINGAN NIRKABEL YANG MENERAPKAN WEP".

---

2 Michael Sutton, 2002.
3 Stewart S. Miller, 2003.

1.2. Perumusan Masalah

Berdasarkan latar belakang masalah penelitian yang telah diuraikan sebelumnya, maka diajukan masalah umum penelitian yaitu :

Bagaimana melakukan audit terhadap celah keamanan pada jaringan nirkabel (*wireless Local Area Network*) yang menerapkan *Wired Equivalent Privacy* (WEP). Terkait dengan hal tersebut, penulis melakukan serangan pada jaringan tersebut, dengan mekanisme pembobolan yang biasa dilakukan oleh *hacker* sehingga kunci WEP dapat di-decrypt dan berhasil masuk ke dalam jaringan tersebut. Dari mekanisme ini, kemudian penulis menerapkan strategi penanganan untuk mengurangi resiko pembobolan tersebut.

1.3. Batasan Masalah

Penelitian dibatasi oleh hal-hal yang terkait dengan kasus-kasus serangan yang memanfaatkan celah keamanan WEP, untuk lebih memfokuskan pada masalah yang akan menjadi penelitian dan bahan analisa dalam pembuatan laporan. Batasan-batasan itu sebagai berikut :

1) Perangkat Lunak (software)

Pemilihan perangkat lunak berperan penting dalam melakukan analisa dan audit celah keamanan WEP. Perangkat lunak ada yang bisa didapat gratis dan ada juga yang harus di beli. Pada penelitian ini penulis akan menggunakan perangkat lunak bebas dan *open source* seperti Kismet, Airsnort, Aircrack, Aireplay, airodump, dan aireplay

2) Standart 802.11

Umumnya standart yang digunakan adalah 802.11b/g, dan untuk membatasi cakupan masalah, penulis hanya melakukan eksperimen dan penelitian menggunakan standart 802.11b. Eksperimen juga dilakukan dengan mekanisme *open-system,* enkripsi WEP 64-bit, dan menggunakan server DHCP. Karena

mekanisme ini lebih banyak digunakan oleh beberapa perusahaan, termasuk perusahaan tempat penulis melakukan penelitian.

3) Celah keamanan pada jaringan nirkabel

Dalam melakukan penelitian ini penulis memanfaatkan beberapa celah keamanan dan strategi yang biasa digunakan oleh *hacker* untuk membobol nirkabel, seperti yang terdefinisikan disini, yaitu :

Pertama, *footprinting*, merupakan kegiatan *scanning* dan *probing* untuk mengetahui celah keamanan pada sebuah jaringan nirkabel.

Kedua, *sniffing*, karena jaringan nirkabel melalui gelombang udara (airwaves), sehingga memudahkan melakukan *Sniffing packet* pada saat terjadi lalu lintas pada jaringan nirkabel.

Ketiga, b*rute-force Attack*, Dikenal sebagai password *cracking* atau *dictionary attack*, tipe ini menggunakan dictionary untuk melakukan *cracking* pada password yang ada. Serangan ini dapat dilakukan sekalipun jaringan tersebut mengimplementasikan authentikasi melalui password.

Keempat, *packet injection* atau *ARP replay*, Metode ini digunakan untuk mempercepat proses *Sniffing*, sehingga jumlah paket yang terkumpul melebihi dari keadaan secara normal. Dan untuk melakukan metode ini penulis menggunakan protokol ARP.

Dari uraian diatas, maka dalam penelitian ini yang menjadi titik perhatian utama adalah melakukan audit celah keamanan WEP pada jaringan nirkabel menggunakan sistem operasi GNU/Linux Ubuntu 6.0.6, dan perangkat lunak *open source* seperti Kismet, Airsnort, Aircrack, Aireplay, dan airodump.

1.4. Maksud dan Tujuan Penelitian

Adapun maksud dan tujuan yang ingin dicapai penulis dalam penulisan skripsi ini terbagi menjadi dua kelompok yaitu :

1.4.1. Maksud

1.4.1.1. Bagi Penulis

a) Untuk memenuhi persyaratan dalam rangka menyelesaikan program studi Strata-1 Teknik Informatika di Sekolah Tinggi Manajemen Informatika dan Komputer AMIKOM Yogyakarta.

b) Menerapkan ilmu pengetahuan yang telah diperoleh penulis di bidang jaringan komputer khususnya tingkat keamanan jaringan.

c) Mengembangkan potensi diri serta membuka wawasan pengetahuan baru sesuai dengan bidang yang saat ini ditekuni, yaitu bagaimana mengaudit celah keamanan pada jaringan nirkabel yang menerapkan WEP.

1.4.1.2. Bagi Pembaca

a) Dapat dipergunakan sebagaimana mestinya yakni sebagai sumber acuan dan referensi dalam penyusunan skripsi.

b) Dapat dipergunakan sebagai media alternatif sumber informasi tentang topik permasalahan yang bersangkutan.

1.4.2. Tujuan

a) Melakukan pembuktian terhadap celah keamanan pada WEP.
b) Melakukan audit pada jaringan nirkabel yang menerapkan WEP.
c) Menentukan solusi yang tepat untuk mengurangi resiko penyerangan yang dilakukan oleh *hacker*.

1.5. Metode Penelitian

Adapun metode penelitian yang digunakan oleh penulis adalah :

a) Metode Observasi

   Yaitu pengumpulan data dengan pengamatan secara langsung pada objek yang diteliti untuk memperoleh informasi yang tepat dan sistematis.

b) Metode Interview

   Yaitu pengumpulan data dengan mengadakan tanya jawab secara langsung dengan responden atau sumber data yang dianggap perlu, bahkan penulis langsung menanyakan hal yang dianggap tidak diketahui dengan mengikuti mailing list dan forum.

c) Metode kepustakaan

   Yaitu pengumpulan data dengan cara membaca berdasarkan kepustakaan yang mana dimaksudkan untuk mendapatkan konsep teori mengenai masalah yang diteliti, serta mencari sumber data dengan mencari di internet dan perpustakaan.

d) Metode eksperimen

   Yaitu melakukan percobaan terhadap objek pada jaringan nirkabel yang menerapkan WEP, melakukan audit terhadap celah keamanan WEP dengan menggunakan strategi yang biasa digunakan oleh pihak ketiga

(*hacker*). Kemudian menentukan solusi yang tepat untuk mengurangi resiko terhadap penyerangan tersebut.

1.6. Sistematika Penulisan

Seperti umumnya laporan penelitian ilmiah, penulisan tesis, maupun disertasi, maka laporan skripsi ini meliputi :

BAB I. PENDAHULUAN

Menguraikan latar belakang masalah, perumusan masalah, batasan masalah, maksud dan tujuan penelitian, metode penelitian, serta sistematika penelitian.

BAB II. TINJAUAN PUSTAKA

Membahas mengenai tinjauan pustaka WEP, dan landasan teori mengenai jaringan nirkabel baik celah keamanannya secara umum maupun beberapa fitur keamanan yang didukung.

BAB III. CARA PENELITIAN

Dalam bab ini dibahas cara penulis melakukan audit WEP dengan menentukan subyek penelitian, alat penelitian, langkah-langkah penelitian dan langkah-langkah pengujian.

BAB IV. HASIL PENGUJIAN DAN PEMBAHASAN

Memberikan hasil analisa dari tool yang digunakan, membahas mengenai cara kerja *hacker* dalam melakukan serangan pada WEP dan solusi untuk mengurangi terhadap serangan tersebut.

BAB V. PENUTUP

Dalam bab ini berisikan kesimpulan dari penelitian dan saran-saran yang ditujukan pada pihak yang terkait.

DAFTAR PUSTAKA

Bagian ini memuat keterangan buku, dan literature lain yang diperoleh dari Majalah, Internet, dan paper penelitian yang menjadi acuan dalam penyusunan skripsi.

1.7. Jadwal Penelitian

Untuk menghasilkan penelitian yang terencana dan penyusunan yang tepat waktu, maka perlu adanya jadwal penelitian. Dalam penelitian ini ada beberapa tahapan kerja yang tersusun dan saling mendukung. Adapun rencana kerja kegiatan di uraikan sebagai berikut.

Tabel.1-1. Jadwal Penelitian

No	Nama Kegiatan	November - Desember				Januari - Februari				Maret - April			
		1	2	3	4	1	2	3	4	1	2	3	4
1.	Persiapan												
2.	Perancangan metode penelitian												
3.	Penelitian dan pengambilan data												
4.	Analisa data												
5.	Pembuatan Laporan												