BAB I
PENDAHULUAN

1. Latar Belakang Masalah

Komunikasi nirkabel telah menjadi kebutuhan dasar atau gaya hidup baru masyarakat informasi. LAN nirkabel yang lebih dikenal dengan jaringan Wi-Fi menjadi teknologi alternative dan relative lebih mudah untuk diimplementasikan di lingkungan kerja (SOHO / *Small Office Home Office*), seperti perkantoran, laboratorium komputer, dan sebagainya. Instalasi perangkat jaringan nirkabel lebih fleksibel karena tidak membutuhkan penghubung kabel antar komputer. Komputer dengan perangkat Wi-Fi dapat saling terhubung yang hanya membutuhkan ruang atau space dengan syarat jarak jangkauan dibatasi kekuatan pancaran sinyal radio dari masing-masing komputer.

Salah satu aspek penting yang harus diperhatikan dengan adanya sistem jaringan komputer nirkabel adalah masalah keamanannya, dimana dengan banyaknya komputer yang dihubungkan dalam suatu jaringan dan banyaknya user yang memakai, suatu data maupun informasi menjadi sangat rentan terhadap serangan-serangan dari pihak-pihak yang tidak berwenang.

Kemudahan instalasi 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.

Dari kelemahan tersebut, ternyata membawa beberapa peneliti dan hacker untuk melakukan analisa untuk membuktikan kelemahan jaringan nirkabel. Sehingga berkembanglah perangkat lunak bebas yang digunakan untuk menunjukkan kelemahan pada sistem keamanan nirkabel WEP dan WPA seperti Aircrack-ng, yang dapat melakukan *recovery* pada kunci yang terenkripsi.

Serangan terhadap jaringan nirkabel pun berkembang. Penyerangan yang dilakukan *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 melakukan audit celah keamanan WEP dan WPA menggunakan cara kerja pihak ketiga (*hacker*) dalam melakukan praktek *hacking*, dalam kasus ini adalah pada jaringan hotspot perusahaan XYZ yang merupakan perusahaan fiktif (bukan sebenarnya) yang mengimplementasikan LAN nirkabel. Dari cara kerja tersebut penulis dapat mengambil langkah penanggulangan terhadap celah tersebut.

Untuk alasan tersebut penulis memilih judul "ANALISIS SISTEM KEAMANAN JARINGAN NIRKABEL (Studi Kasus pada Jaringan Hot-Spot PT. XYZ yang Menerapkan WEP dan WPA-PSK)".

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) dan *Wi-fi Protected Access* (WPA-PSK). Terkait dengan hal tersebut, penulis melakukan serangan pada jaringan hot-spot PT. XYZ, dengan mekanisme pembobolan yang biasa dilakukan oleh *hacker* sehingga kunci WEP dan WPA-PSK dapat di-*decrypt* dan berhasil masuk ke dalam jaringan tersebut. Dari mekanisme ini, kemudian penulis menerapkan strategi penanganan untuk mengurangi resiko pembobolan tersebut.

3. Batasan Masalah

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

a. Jaringan Hostpot pada PT. XYZ

Dalam melakukan penelitian ini penulis mencoba melakukan analisa dan audit pada jaringan Hostpot PT. XYZ, dimana perusahaan ini merupakan perusahaan fiktif yang menyediakan jaringan hostpot dengan menggunakan keamanan WEP dan WPA-PSK. Penulis melakukan audit dan penelitian pada jaringan yang penulis bangun sendiri dengan berusaha mengimplementasikan seperti yang biasa diimplementasikan pada perusahaan secara sederhana yang tidak menggunakan sistem keamanan tingkat lanjut seperti RADIUS.

b. Perangkat Lunak (*Software*)

Pemilihan perangkat lunak berperan penting dalam melakukan analisa dan audit celah keamanan jaringan nirkabel. Perangkat lunak ada yang bisa didapat secara gratis dan ada juga yang harus dibeli. Pada penelitian ini penulis akan menggunakan perangkat lunak bebas dan *open source* seperti Kismet, Airodump-ng, Aireplay-ng, Aircrack-ng, Aircrack-ptw, dan Wireshark yang semuanya sudah terangkum dan terdapat pada sebuah distribusi linux Live CD bernama Backtrack 2. Kecuali untuk software Aircrack-ptw ditambahkan dan dicompile ulang kedalam CD oleh komunitas kemanan jaringan "Jasakom" yang kemudian diberi nama Backtrack 2+.

c. Strategi Hacking

Dalam melakukan penelitian ini penulis memanfaatkan beberapa celah keamanan dan strategi yang biasa digunakan oleh *hacker* untuk membobol jaringan 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, *packet injection* atau *ARP replay,* metode ini digunakan untuk mempercepat proses *sniffing*, sehingga jumlah paket yang terkumpul melebihi dari keadaan normal. Dan untuk melakukan metode ini penulis menggunakan protokol ARP.

Keempat, *brute-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.

4. Maksud dan Tujuan Penelitian

Adapun maksud dan tujuan yang ingin dicapai penulis dalam penulisan skripsi ini yaitu:

Maksud

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

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

c) Dapat dipergunakan untuk memahami pentingnya keamanan jaringan dalam hal ini jaringan nirkabel yang setiap saat terus berkembang.

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

Tujuan

a) Melakukan pembuktian terhadap celah kemanan pada WEP dan WPA-PSK.

b) Melakukan audit pada jaringan nirkabel yang menerapkan WEP dan WPA-PSK.

c) Menentukan solusi yang tepat untuk mengurangi resiko penyerangan yang dilakukan oleh *hacker*.

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 Kepustakaan

Yaitu pengumpulan informasi dan 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.

c) 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.

d) Metode Eksperimen

Yaitu melakukan percobaan terhadap objek pada jaringan nirkabel yang menerapkan WEP dan WPA-PSK, melakukan audit terhadap celah keamanan jaringan tersebut dengan menggunakan strategi yang biasa digunakan oleh pihak ketiga (*hacker*). Kemudian menentukan solusi yang tepat untuk mengurangi resiko terhadap penyerangan tersebut.

6. Sistematika Penulisan

Seperti umumnya laporan penelitian, 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. LANDASAN TEORI

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

BAB III. RANCANGAN DAN KONFIGURASI

Dalam bab ini dibahas cara penulis melakukan audit WEP dan WPA-PSK dengan menentukan rancangan dan konfigurasi subjek 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 WPA-PSK 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 literatur lain yang diperoleh dari Majalah, Internet, dan paper penelitian yang menjadi acuan dalam penyusunan skripsi.

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 kegiatan diuraikan sebagai berikut.

Tabel.1-1. Jadwal Penelitian

No	Rincian Tahap Kerja	Bulan											
		November				Desember				Januari			
		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												