BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Jaringan komputer telah menjadi sebuah aspek yang sulit dipisahkan dari dunia komputer. Jaringan komputer, seperti halnya dunia komputer pada umumnya, mengalami perkembangan yang cukup berarti. Awalnya untuk menghubungkan beberapa komputer digunakan teknologi kabel (*wired*). Komputer-komputer yang terhubung dengan kabel ini membentuk sebuah jaringan komputer (*Local Area Network*). Kemudian berkembang teknologi jaringan komputer yang tidak menggunakan kabel (*wireless*). Penggunaan teknologi jaringan tanpa kabel ini kemudian memunculkan istilah baru yaitu *Wireless Local Area Network* (WLAN).

WLAN memiliki beberapa keunggulan dibandingkan LAN antara lain dari segi kenyamanan, produktivitas, mobilitas dan harga. Mayoritas komputer atau *laptop* yang diperdagangkan sekarang telah dilengkapi dengan sarana untuk mendukung WLAN. Walau begitu, WLAN juga memiliki beberapa kekurangan, seperti kecepatan, realibilitas dan keamanan. Keamanan menjadi isu penting dalam sebuah jaringan, terutama WLAN. Hal ini disebabkan karena dari awal koneksi sebuah perangkat ke sebuah jaringan WLAN, telah diadakan pertukaran paket untuk proses autentikasi dan juga pada jaringan proses pertukaran data menjadi sebuah kegiatan yang cukup sering dilakukan. Untuk memperbaiki sisi

keamanan WLAN, maka diciptakanlah metode-metode keamanan khusus untuk WLAN. Salah satu metode keamanan yang banyak diimplementasikan pada WLAN adalah *Wired Equivalency Privacy* (WEP). Walau begitu, karena kelemahan dari metode ini maka dibuatlah metode keamanan baru yang disebut dengan *Wi-Fi Protected Access* (WPA).

Penelitian ini berpusat pada proses bagaimana seorang *hacker* menembus WLAN terutama yang menggunakan metode keamanan WPA. Pada umumnya kegiatan *hacking* diawali dengan mengamati jaringan untuk mendapatkan informasi yang diperlukan agar *hacker* dapat menyusup ke dalam jaringan. Penelitian akan menunjukkan bagaimana seorang *hacker* dapat mengamati WLAN, mengambil paket *handshaking*, mendapatkan WPA *keys*, hingga akhirnya berhasil masuk ke dalam WLAN.

Dengan penelitian ini juga diperlihatkan bagaimana kemampuan WLAN dengan metode keamanan WPA dapat bertahan dari serangan *hacker*. Pada penelitian ini digunakan sistem operasi Linux *BackTrack* 2.0. Penggunaan sistem operasi ini didasarkan pada pertimbangan bahwa *BackTrack* merupakan *distro* Linux yang biasa dipakai oleh para *hacker* jaringan. *Distro* ini juga dapat memfungsikan WLAN *card* tertentu untuk melakukan pendeteksian protokol WLAN dan *BackTrack* 2.0 bisa didapatkan dengan cuma-cuma.

1.2. Perumusan Masalah

Tujuan penulisan tugas akhir ini adalah untuk mengetahui tingkat keamanan pada WPA dengan cara melakukan serangkaian percobaan untuk mendukung kesimpulan yang ditulis pada akhir penulisan tugas akhir ini. Penelitian ini dilakukan juga untuk mendapatkan kunci yang terdapat pada *access point*, menganalisis kelemahan yang terdapat pada WPA, dan menawarkan solusi praktis untuk mengatasi kelemahan yang ada.

1.3. Pembatasan Masalah

Ruang lingkup penelitian kali ini mencakup:

1. Kegiatan penyerangan *access point* WLAN menggunakan metode keamanan WPA dan juga teori penyerangan terhadap WPA.
2. Penggunaan *hardware*, dalam hal ini *laptop*, menggunakan sistem operasi Linux dengan *distro BackTrack* 2.0 sebagai alat *hacking* dan sebuah *wireless router* yang telah menggunakan metode keamanan WPA sebagai target penyerangan.
3. Penggunaan *BackTrack* 2.0 dalam penyerangan.
4. Analisis pada saat penyerangan terjadi dan tindakan pencegahan terhadap penyerangan.

1.4. Tujuan Penelitian

Tujuan penelitian ini adalah :

1) Mempelajari sistematika serangan *hacker* terhadap WLAN dengan modus keamanan WPA.
2) Melakukan percobaan *hacking* untuk dapat mendukung sistematika serangan tersebut.
3) Memberikan beberapa solusi yang dapat mengurangi kemungkinan penyerangan berhasil.

1.5.Metodologi Penelitian

Metode penelitian yang penulis pakai adalah metode penelitian studi literatur dan eksperimental, yang bertujuan untuk memperkaya pengetahuan tentang keamanan jaringan komputer, melalui metode yang menjadikan komputer sebagai obyek kajian. Adapun langkah-langkah yang digunakan untuk mendukung penelitian adalah dengan melakukan:

1) Studi literatur lewat buku ataupun artikel.
2) Melakukan instalasi *BackTrack* 2.0.
3) Mempelajari sistem operasi Linux khususnya *distro BackTrack* 2.0.
4) Mempelajari *tools* yang terdapat di *BackTrack* 2.0 untuk melakukan *hacking.*
5) Mempelajari sistematika *hacking* WLAN.
6) Melakukan percobaan *hacking.*
7) Menganalisis *hacking* yang telah dilakukan.

8) Mengusulkan solusi praktis.

9) Penulisan laporan tugas akhir.

1.6. Sistematika Penulisan

Penulisan Laporan Tugas Akhir meliputi pembagian bab sebagai berikut:

Bab I Pendahuluan

Bab ini meliputi latar belakang masalah yang berhubungan dengan judul tugas akhir, pokok permasalahan yang menjelaskan permasalahan dalam judul, pembatasan masalah yang merupakan batasan yang dibuat dalam laporan dan aplikasi, tujuan penelitian, dan sistematika penulisan.

Bab II Landasan Teori

Bab ini meliputi teori-teori pendukung yang dibutuhkan dalam penelitian dan penyusunan laporan tugas akhir ini. Teori-teori pendukung didapatkan dari studi literatur dari perpustakaan dan *internet*.

Bab III Perancangan Penyerangan

Bab ini menjelaskan proses penyerangan yang akan dilakukan, informasi yang dibutuhkan untuk melakukan penyerangan, serta proses penyerangan hingga mendapatkan *pre-shared key* dari WPA.

Bab IV Implementasi Penyerangan dan Tindakan Pencegahan

Bab ini menjelaskan hasil penyerangan yang telah dirancang pada bab sebelumnya, analisis serangan yang dilakukan dan tindakan pencegahan serangan.

Bab V Kesimpulan dan Saran

Bab ini terdiri dari kesimpulan yang didapat dari penelitian dan juga saran yang bertujuan untuk mengembangkan WLAN yang lebih baik dalam hal pertahanan terhadap *hacker*.