BAB I
PENDAHULUAN

1.1 Latar Belakang

Di era modern saat ini sangat identik dengan efisiensi dan juga inovasi dalam semua aspek pada bidang kehidupan, perkembangan teknologi informasi dan komunikasi menjadi suatu keharusan. Teknologi informasi dan komunikasi merupakan salah satu hal yang sangat sulit untuk dipisahkan dari kehidupan manusia itu sendiri di era modern yang bergerak dengan cepat saat ini. Salah satu dari sekian banyaknya contoh kemajuan teknologi informasi dan komunikasi yaitu *Wireless Local Area Network* (WLAN) atau biasa disebut juga dengan teknologi jaringan lokal nirkabel.

Penggunaan dari teknologi *wireless* sendiri sudah sering dijumpai pada *Cafe, hotspot* komersil, kampus, perkantoran serta tempat-tempat umum, tetapi sangat sedikit yang memperhatikan sistem dari keamanan komunikasi data pada sebuah jaringan *wireless*. Padahal pada praktiknya dalam membangun perancangan, sebuah sistem keamanan jaringan yang terhubung ke internet seharusnya direncanakan dan dipahami dengan sangat baik agar dapat melindungi sumber daya yang sedang berada dalam jaringan tersebut dan juga dapat meminimalisir terjadinya serangan yang dilakukan oleh orang yang tidak bertanggung jawab.

Kelemahan jaringan *wireless* secara umum bisa dibagi menjadi 2 jenis, yaitu kelemahan pada konfigurasi dan kelemahan pada jenis enkripsi yang digunakan. Salah satu metode yang dapat digunakan dalam mengevaluasi sebuah jaringan adalah dengan melakukan pengujian secara langsung terhadap sistem dengan mensimulasikan bentuk-bentuk serangan terhadap jaringan atau yang sudah biasa disebut dengan metode *Penetration testing*[1].

Untuk dapat melihat kualitas keamanan pada jaringan diperlukan analisa terhadap sistem keamanan yang ada dalam jaringan tersebut. Salah satu metode yang bisa digunakan untuk mengevaluasi jaringan yaitu metode *Penetration Testing,* dengan cara melakukan pengujian terhadap sistem dengan mensimulasikan bentuk-bentuk serangan terhadap jaringan.

Dalam menganalisis keamanan jaringan dengan menggunakan metode *Penetration testing* dengan bentuk serangan terhadap jaringan yang disimulasikan, salah satu sistem operasi yang memiliki spesifikasi yang tepat dalam hal tersebut adalah Kali Linux. Karena Kali Linux berbeda dari distro Linux yang lain, semisal Ubuntu yang lebih mengutamakan aspek *user friendly* dan *balancing*, Kali Linux sudah dirancang dengan khusus untuk melakukan pengujian keamanan jaringan, dengan dilengkapi dengan aplikasi pendukung yang digunakan dalam aktivitas *hacking* dan memanfaatkannya sebagai alat pengujian untuk keamanan jaringan.

IT Telkom Purwokerto merupakan salah satu kampus yang menggunakan teknologi WLAN untuk berbagai keperluan yang bersifat akademik, baik oleh mahasiswa, pegawai maupun Dosen. Pengunaan teknologi WLAN sendiri di samping mempermudah di bidang akademik, juga dapat disalah gunakan oleh orang-orang yang tidak bertanggung jawab, apabila tanpa adanya pencegahan untuk mengetahui celah yang dapat dimanfaatkan untuk melakukan tindakan *hacking* yang dapat mengakibatkan kerugian. Untuk mengetahui keamanan jaringan WLAN maka diperlukan adanya sebuah uji coba pada jaringan tersebut yang berguna untuk mengetahui celah atau kerentanan. Hasil dari uji coba nantinya dapat digunakan sebagai pertimbangan untuk menentukan jaringan yang tersedia sudah cukup aman atau masih perlu untuk ditingkatkan keamanannya.

Berdasarkan uraian di atas, penulis mengangkat permasalahan jaringan WLAN di IT Telkom Purwokerto untuk dilakukan penelitian dengan judul "**Analisis Keamanan Pada Jaringan WLAN Menggunakan Metode *Penetration Testing* (Studi Kasus: Jaringan IT Telkom Purwokerto)**".

1.2 Rumusan Masalah

Dengan berdasarkan latar belakang yang telah diuraikan di atas, dapat dirumuskan masalah yang berkaitan dengan penelitian yang akan dilakukan yaitu belum adanya penelitian tentang keamanan jaringan WLAN di IT Telkom Purwokerto menggunakan metode *Penetration Testing* yang berfungsi untuk menemukan celah atau kerentanan pada jaringan yang tersedia.

1.3 Tujuan Penelitian

Tujuan penelitian yang hendak dicapai oleh penulis dalam penelitian ini adalah untuk menganalisis keamanan jaringan WLAN yang tersedia di IT Telkom Purwokerto dengan menggunakan metode *Penetration Testing.*

1.4 Batasan Masalah

Berdasarkan rumusan masalah dan tujuan penelitian, maka untuk mewujudkan penelitian yang sesuai dengan masalah yang ada diperoleh batasan-batasan masalah penelitian sebagai berikut:

1. Penggunakaan *tools* seperti *Burpsuite, Wireshark, Netdiscover, Hping3* dan *Ettercap* untuk mencari celah keamanan jaringan di IT Telkom Purwokerto.
2. Pengujian dilakukan di Laboratorium Pemrograman IT Telkom Purwokerto dengan cara melakukan simulasi menggunakan dua peran yaitu komputer yang berperan sebagai penyerang dan juga korban.
3. Penulis hanya melakukan analisis keamanan jaringan dan tidak melakukan implementasi peningkatan keamanan jaringan.

1.5 Manfaat Penelitian

Manfaat penelitian dalam penyusunan tugas akhir ini adalah:

1. Manfaat bagi peneliti, dapat menerapkan metode *penetration testing* untuk menganalisis keamanan sebuah jaringan.
2. Manfaat bagi akademik, diharapkan tugas akhir ini dapat dijadikan perbandingan untuk penelitian serupa.
3. Manfaat bagi kalangan umum, diharapkan tugas akhir ini dapat bermanfaat dan dipertimbangkan untuk dikembangkan lebih lanjut.