# BAB I

# PENDAHULUAN

## 1.1. Latar Belakang Penelitian

Jaringan komputer telah mengalami perkembangan yang pesat. Seiring dengan munculnya infrastruktur jaringan nirkabel, perlahan jaringan berbasis kabel mulai ditinggalkan. Kebutuhan pengguna jaringan yang terus meningkat membuat penggunanya ingin menggunakan sebuah koneksi yang bisa digunakan dimana saja dan kapan saja.

Teknologi nirkabel saat ini berkembang sangat pesat terutama dengan hadirnya perangkat teknologi informasi dan komunikasi. Perangkat seperti *Smartphone,* tablet, laptop mendominasi pemakaian jaringa nirkabel ini. Penggunakan jaringan nirkabel yang diimplementasikan dalam jaringan local sering dinamakan WLAN (*Wireless Local Area Network*).

Jaringan nirkabel ini juga populer dengan istilah Wi-Fi atau *Wireless Fidelity* . Wi-fi memiliki beragam standar 802.11 yang ditetapkan oleh Institude of Electrical and Electronics Engineer (IEEE). Untuk konensi Wi-fi antar perangkat, ada tiga jenis jaringan nirkabel yang ditetapkan oleh IEEE. Standarnya adalah jaringan 802.11a, 802.11b, dan 802.11g. yang membedakan masing-masing standarnya adalah jangkauan frekuensi dan kecepatan transfernya (Maslan & Wangdra, 2012:103).

Peningkatan jumlah pengguna *smartphone* didunia sangatlah mengesankan. Ada pertumbuhan pesat pengguna yang menggunakan Wi-fi melalui *smartphone*. Perangkat khusus seperti Tablet hanya terhubung melalui Wi-fi. Semua perangkat ini terhubung ke jaringan nirkabel melalui perangkat yang disebut *Wireless Access Point* (WAP). *Access Point* (AP) sangatlah populer karena fiturnya seperti mudah dipasang, hemat biaya, mudah dikonfigurasi, dan yang lebih penting memberikan mobilitas.

Penggunaan Wi-Fi publik telah mencapai pada tingkat yang sulit dihindari. Perusahaan Kaspersky melakukan pemungutan suara secara global melalui Facebook pada tahun 2013 tentang keamanan jaringan nirkabel, dan hasilnya menunjukkan bahwa lebih dari 42% pengguna mengatakan bahwa mereka menggunakan Wi-Fi umum tanpa mempertimbangkan keamanannya. Seorang *Hacker* (Penyerang) dapat membuat AP tiduran dilingkungan nirkabel. Sasaran utama penyerang ini ada mengganggu jaringan dan mencoba mencuri informasi sensitif seperti penggunakan E-Banking pada jaringan nirkabel umum.

Jika AP palsu tidak terdeteksi maka membuka cela bagi penyerang untuk mendapatkan infomrasi yang sensitif. Penyerang mengambil keuntungan dari AP yang tidak terdeteksi untuk mendapatkan internet gratis, informasi rahasia. Jika AP palsu ditambahkan kejaringan, itu harus ditemukan dan tindakan yang diperlukan harus dilakukan untuk memperbaiki situasi. Menurut hasil laporan perusahaan AirTight Networks atau juga dikenal dengan Mojo Networks, 20% dari total AP yang ada, adalah AP palsu dan pengguna dapat dengan mudah-terhubung ke AP ini karena kurangnya pengetahuan tentang ancaman keamana di WLAN.

AP palsu mudah disebarkan, sulit dideteksi, dan membuka peluang terhadap jaringan akan berbagai serangan. Ini melakukan dua jenis serangan, yaitu pasif dan aktif. Dalam serangan pasif, penyerang tidak mempengaruhi perilaku normal jaringan. Bahkan pengguna jaringan tidak menyadari akan serangan tersebut. Penyerang mencuri informasi rahasia tanpa mengetahui pengguna saat dalam serangan aktif. Penyerang mempengaruhi perilaku normal jaringan. Serangan aktif yang paling umum adalah *Denial of Service*, Serangan *Man-in Middle* dan serangan *Evil Twin Attack* atau biasa juga di sebut dengan *Rouge Access Point.*

IEEE 802.11 memungkinkan pendistribusian yang murah dan bisa digunakan untuk menutupi area di mana kabel tidak bisa digunakan, karena banyak digunakan dikantor-kantor perusahaan, kampus perguruan tinggi dan untuk rumahan. Bahkan, WLAN sangat meningkatkan produktivitas dan keramahan dengan menyediakan akses kapan saja dan di mana saja. Ini meningkatkan kerentanan dari WLAN dimanfaatkan oleh para penyerang . Ada beberapa alasan jaringan nirkabel menjadi mudah untuk diserang. Pertama, mudah terpengaruh oleh media transmisi misalnya udara. Kedua, pola enkripsi yang lemah seperti WEP, WPA dan WPA2 yang bisa ditembus (dipenetrasi) dengan menggunakan tool seperti Backtrack dan Aircrack. Ketiga, *wireless interface device* pada jaringan nirkabel memiliki alamat MAC (*Medium Access Control*) unik yang mana dapat dipalsukan oleh Hakcer dan dapat digunakan untuk menukar identitas tiduran *Access Point* (AP) sebagai AP yang asli.

Dengan peningkatan perataan jaringan Wi-Fi, mengamankan jaringan menjadi sebuah masalah yang menggugah pikiran. Diantara semua ancaman keamanan, satu dari bahaya yang paling mengancam adalah pemerataan pemalsuan

AP. Sebuah AP palsu mengartikan sebagai AP yang tidak diberi kekuasaan atau AP penipu.

Tingkat keamanan wifi lebih rendah dibandingkan dengan jaringan berbasis kabel, karena hacker tidak perlu melakukan koneksi secara fisik. Lemahnya kesadaran pengguna dalam mengawasi keamanan jaringannya memberikan kesempatan para hacker untuk menyelusup. Dengan semakin banyaknya jaringan nirkabel dan sensor jaringan yang didistribusikan, hal tersebut menjadi sasaran yang menarik bagi para penyerang. Karena keterbukaan jaringan nirkabel dan sensor jaringan, Serangan *Spoofing* sangat mudah untuk dijalankan. Serangan spoofing berarti penempaan identitas seseorang, yang mana biasanya pengguna yang terdaftar dan dengan demikian mendapatkan akses data admin. Serangan *Spoofing* (*Spoofing Attack*) merupakan sebuah serangan yang serius karena membahayakan identitas dan juga serangkaian serangan-serangan lainnya seperti *evil twin access point attack.*

Ada beberapa metode yang biasanya digunakan oleh *hacker* dalam melakukan penyerangan terhadap suatu AP seperti metode *Brute Force*, yaitu suatu jenis serangan yang dilakukan dengan cara mencoba login berulang-ulang menggunakan segala kemungkinan kata sandi (*password*) yang ada. *Password* tersebut biasanya berupa text berisi ribuan baris password yang disebut dengan *wordlist*. Berbeda dengan metode *brute force*, yang dimana penyerang murni mengandalkan keahlian penyerang dalam mengumpulkan informasi, menunggu dan menebak, *evil twin attack* sangat tergantung pada keledoran korban dalam menggunakan jaringan nirkabel. Seperti dengan nama metodenya, *Evil Twin* adalah

teknik penyerangan jaringan nirkabel dengan cara membuat kembaran *access point*. Hal tersebut menyebabkan komputer korban menangkap dua sinyal dengan SSID (*Service Set Identifier)* yang sama. Disinilah letak kelemahan sistem. Tiap komputer hanya mengingat SSID dan menyambung otomatis jika *connect automaticly* nya diaktifkan. Jika ada dua SSID yang sama, maka sinyal terkuatlah yang akan terhubung. Secara teori, korban harus lebih dekat dengan penyerang dibandingkan AP aslinya.

Berdasarkan permasalahan yang ada diatas, penulis bermaksud melakukan penelitian dengan judul "**ANALISIS DAN PENGUJIAN KELEMAHAN KEAMANAN JAIRNGAN NIRKABEL DENGAN *METODE EVIL TWIN ATTACK* PADA KALI LINUX**" untuk melakukan pengujian terhadapat keamanan jaringan nirkabel yang digunakan di tempat-tempat umum seperti cafe di mall-mall di kota Batam. Oleh karena itu penulis ingin membuat penjabaran mengenai analisis dan pengujian jaringan nirkabel menggunakan metode *Evil Twin Attack* pada Kali Linux agar masyarakat pengguna mengetahui betapa pentingnya suatu pengamanan pada jaringan nirkabel.

## 1.2. Identifikasi Masalah

Berdasarkan latar belakang penelitan diatas, ada beberapa masalah yang teridentifikasi, yaitu sebagai berikut :

1. Penggunaan jaringan nirkabel yang meluas menigkatkan celah keamanan bagi para *Hacker*.

2. Alamat MAC (*Medium Access Control*) pada *Wireless Interface Device* yang dapat dipalsukan oleh Hacker dan dapat digunakan untuk menukar identitas tiruan *Access Point* (AP) sebagai AP yang asli.
3. Penggunaan metode *Evil Twin Attack* yang dapat dilakukan untuk mendapatkan akses pada suatu jaringan nirkabel.

## 1.3. Pembatasan Masalah

Untuk mencegah meluasnya ruang lingkup pembahasan, maka penulis memberikan pembatasan masalah pada penelitian ini, sebagai berikut :

1. Pengujian dilakukan pada jaringan nirkabel 1 buah cafe yang dipilih secara random di, Nagoya Hill Mall, Kepri Mall, dan Mega Mall di Kota Batam.
2. Pembahasan meliputi analisis dan pengujian keamanan jaringan nirkabel dengan menggunakan metode *Evil Twin Attack* pada Kali Linux.

## 1.4. Perumusan Masalah

Berdasarkan identifikasi masalah diatas, Maka perumusan masalah dalam penelitian ini adalah :

1. Bagaimana cara memperkuat keamanan jaringan nirkabel ?
2. Bagaimana cara mencegah *Hacker* untuk tidak memalsukan alamat MAC serta *Access Point* ?
3. Bagaimana cara pengujian keamanan jaringan nirkabel dengan metode *Evil Twin Attack* ?

## 1.5. Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah sebagai berikut :

1. Untuk meningkatkan keamanan jaringan nirkabel yang digunakan secara publik.
2. Untuk mencegah *Hacker* mendapatkan akses dan informasi dari jaringan nirkabel publik.
3. Untuk menganalisis dan menguji keamanan suatu jaringan nirkabel.

## 1.6. Manfaat Penelitian

Adapun manfaat yang diharapkan setelah tujuan diatas dapat dicapai adalah sebagai berikut :

### 1.6.1. Manfaat Teoritis

Memberikan gambaran tingkat keamanan jaringan nirkabel yang bisa di terapkan pada saat ini, sehingga dapat memberikan petunjuk untuk menghindari sistem keamanan yang lemah.

### 1.6.2. Manfaat Praktis

Hasil penelitian ini diharapkan dapat memberikan informasi yang bermanfaat mengenai keamanan jaringan pada masyarakat umum.