# BAB I

# PENDAHULUAN

## 1.1 Latar Belakang

WPA dan WPA2 merupakan protokol otentikasi yang digunakan untuk kemanan jaringan nirkabel. WPA menyediakan kunci yang berbeda untuk setiap pengguna namun dapat menggunakan mode kunci yang di bagikan sebelumnya (PSK). Data dienkripsi menggunakan algoritma *cipher* RC4 yang menggunakan 128-bit kunci dan 48-bit inisial vektor. Salah satu peningkatan terbesar dari protokol sebelumnya WEP adalah WPA mengandung algoritma TKIP yang dimana secara dinamis mengubah kunci saat sistem digunakan. Algoritma tambahan yang digunakan WPA adalah MIC digunakan untuk mengecek integritas data serta untuk mengatasi kelemahan protokol sebelumnya yang memakai CRC. Kelebihan MIC dibandingkan CRC adalah mekanisme penghitung *frame* yang digunakan untuk mencegah eksekusi serangan secara berulang.

Ada banyak kesamaan antara WPA2 dan WPA dalam hal keamanan otentikasi. Perbedaan dari kedua protokol ini adalah WPA2 menggunakan algoritma AES, sedangkan WPA yang sebelumnya sudah disebutkan menggunakan TKIP. AES adalah sandi blok simetris yang digunakan untuk melindungi informasi rahasia dan diimplementasikan kedalam perangkat lunak dan perangkat keras untuk mengenkripsi data sensitif.

Diantara banyak keunggulan dan keuntungan yang ada, baik WPA maupun WPA2 mempunyai beberapa kelemahan. Jika klien terkoneksi dengan akses poin yang menggunakan kata sandi yang lemah maka pembobolan kata sandi itu sangat memungkinkan. WPA menggunakan kata sandi agar dapat diakses oleh klien. Ketika perangkat terkoneksi ke akses poin dengan kata sandi WPA yang lemah, maka akan mudah terangkap oleh seseorang yang mendengarkannya atau mengendusnya dalam jaringan nirkabel. Menangkap sebuah data bukan masalah besar jika kata sandi yang terenkripsi sangat lemah, maka hanya diperlukan *dictionary attack* yang kemungkinan akan berhasil.

Kelemahan lain yang ada di dalam protokol ini adalah serangan *4-Way handshake* jenis *deauthentication* dan PMKID. *Deauthentication* adalah jenis serangan yang dijalankan ketika klien telah bergabung ke jaringan WI-FI yang dilindungi, dan digunakan untuk mengonfirmasi bahwa klien dan akses poin memiliki kradensial yang benar, contohnya kata sandi yang dibagikan sebelumnya sebelum terhubung ke jaringan. PMKID adalah jenis serangan baru yang tidak tergantung pada klien yang terhubung pada jaringan. Tidak ada interaksi antara penyerang dan klien tetapi hanya antara penyerang dan akses poin. Serangan ini dilakukan pada RSN IE (elemen informasi jaringan keamanan) dari satu *frame* EAPOL.

Dengan adanya permasalahan ini penelitian dilakukan untuk mengetahui bagaimana proses terjadinya serangan terhadap protokol otentikasi WPA dan WPA2, serta solusi pencegahan terhadap jenis serangan yang menggunakan metode *4-Way handshake* dan PMKID di dalam jaringan nirkabel.

## 1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dikemukakan maka permasalahan yang dapat dirumuskan adalah :

1. Bagaimana proses terjadinya serangan *4-Way Handshake* terhadap protokol WPA dan WPA2?
2. Bagaimana proses terjadinya serangan PMKID terhadap protokol WPA dan WPA2?
3. Bagaimana solusi pencegahan terhadap serangan *4-way handshake* dan PMKID pada jaringan nirkabel?

## 1.3 Batasan Masalah

Untuk mendapatkan arah dan tujuan yang baik dan tidak terlalu menyimpang, maka masalah akan dibatasi sebagai berikut :

1. Penelitian menggunakan *tools* Aircrack dan Hashcat yang terinstal pada (OS Kali Linux Ver. 2019.3) untuk melakukan penyerangan terhadap protokol WPA dan WPA2 yang telah dikonfigurasikan pada router Mikrotik RB931-2nd.
2. Jenis enkripsi yang digunakan penelitian adalah enkripsi TKIP dan AES dengan menggunakan mode PSK.
3. Penelitian difokuskan pada proses terjadinya serangan *4-Way Handshake* dan PMKID serta menganalisis serangan mana yang lebih efektif dengan menggunakan *tools* Wireshark.

4. Penelitian tidak menggunakan tambahan *firewall* selain algoritma enkripsi.
5. Akses poin menggunakan protocol DHCP untuk membagikan alamat IP kepada klien.
6. Penerapan keamanan jaringan yang menghubungkan antara klien dan akses poin dilakukan terbatas.

## 1.4 Maksud dan Tujuan Penelitian

Maksud dan tujuan penelitian dari Penelitian dengan judul "Analisis Vulnerability Keamanan Jaringan Wireless Pada Protokol WPA dan WPA2 Terhadap serangan Aircrack/Hashcat Menggunakan Metode 4-Way Handshake Dan Pairwise Master Key Identifier" adalah.

1. Untuk mengetahui proses terjadinya serangan terhadap sebuah jaringan nirkabel dan untuk mengembangkan kualitas jaringan di masa mendatang.
2. Untuk mengetahui proses terjadinya serangan terhadap WPA dan WPA2 yang menggunakan metode serangan 4-*Way Handshake* dan PMKID.
3. Untuk mengetahui jenis serangan mana yang lebih efektif dan efisien dalam melakukan serangan pada protokol WPA dan WPA2
4. Menerapkan pencegahan terhadap serangan 4-*Way Handshake* dan PMKID.

## 1.5 Manfaat Penelitian

Manfaat dari peneliatan yang dibuat adalah :

1. Mahasiswa mampu membuat sebuah kemanan jaringan nirkabel dan melakukan analisis terhadap jaringan tersebut.
2. Mahasiswa mengetahui alur terjadinya serangan *4-Way Handshake* dan PMKID, agar dapat melakukan pencegahan terhadap serangan tersebut.
3. Memperkuat keamanan sebuah jaringan nirkabel untuk meminimalisir serangan yang kemungkinan terjadi.

## 1.6 Metodologi Penelitian

Metodologi yang digunakan dalam penelitian ini adalah :

1. Studi Pustaka

   Mengumpulkan literature berupa teori-teori seperti: jurnal, buku, dan artikel-artikel yang berhubungan dengan penelitian yang dilakukan.

2. Eksperimen

   Membuat dan merancang sebuah jaringan nirkabel kemudian melakukan pengamatan terhadap proses terjadinya serangan *4-Way Handshake* dan PMKID.

## 1.7 Sistematika Penulisan

Dalam penelitian ini penulis membuat sistematika penulisan kedalam beberapa bab dengan rincian sebagai berikut :

BAB I PENDAHULUAN

Bab ini berisi latar belakang, rumusan masalah, batasan masalah, maksud dan tujuan, metodologi penilitian, dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini akan membahas dasar-dasar teori yang digunakan dalam penelitian dan mendukung pelaksanaan penelitian.

BAB III METODE PENELITIAN

Bab ini akan membahas mengenai pemaparan yang digunakan dalam pengumpulan data.

BAB IV ANALISIS DAN PEMBAHASAN

Bab ini akan membahas proses analisis bagaimana terjadinya serangan *4-Way Handshake* dan PMKID terhadap WPA dan WPA2 yang menggunakan algoritma TKIP dan AES. Selain itu bab ini akan membahas tentang monitoring serta pencegahan serangan yang dilakukan terhadap jaringan nirkabel.

BAB V PENUTUP

Bab ini berisi kesimpulan dan saran dari penulis berdasarkan hasil analisis yang ada untuk meningkatkan keamanan jaringan terutama jaringan nirkabel yang menggunakan protokol otentikasi WPA dan WPA2.