

BAB I

PENDAHULUAN

1.1 Latar Belakang

Pada era digital yang semakin berkembang pesat seperti saat ini, tentunya banyak juga yang sudah berubah dari segi kemajuan peralatan dan kemajuan media dalam mencari informasi. Dalam mencari atau menyebarkan informasi pada saat ini dan dulu sungguh sangat berbeda, di era dulu kita masih menggunakan surat kertas dalam menyebarkan informasi, namun di era digital seperti sekarang kita bisa menggunakan media internet. Menggunakan media internet tentunya kita diperkenalkan dengan jaringan internet. konektivitas nirkabel telah menjadi salah satu aspek paling krusial dalam kehidupan sehari-hari. Inovasi teknologi yang paling mencolok adalah jaringan WiFi (Wireless Fidelity). Jaringan WiFi memungkinkan individu dan organisasi untuk terhubung ke internet atau jaringan lokal tanpa perlu tergantung pada kabel fisik yang cenderung kaku dan membatasi mobilitas. Kemudahan dan fleksibilitas yang ditawarkan oleh teknologi WiFi menjadikannya pilihan utama di berbagai setting, seperti rumah tangga, lingkungan kantor, toko, kafe, dan bahkan di tempat-tempat umum seperti bandara dan pusat perbelanjaan.

Namun, seiring dengan kemudahan dan kenyamanan yang ditawarkan oleh jaringan WiFi, muncul pula berbagai perhatian terkait keamanan. Jaringan WiFi sering digunakan untuk mengirimkan informasi yang sangat sensitif, termasuk data pribadi, informasi keuangan, dan data bisnis. Keberadaan informasi ini di udara membuatnya menjadi sasaran potensial bagi para penyerang yang mencari cara untuk mencuri, mengganggu, atau memanipulasi data ini. Oleh karena itu, pengembang jaringan dan pemilik jaringan WiFi harus memastikan bahwa jaringan mereka aman dari ancaman potensial [1].

Protokol keamanan adalah langkah pertama dalam melindungi jaringan WiFi dari ancaman keamanan. Salah satu protokol keamanan WiFi yang paling dikenal dan banyak digunakan adalah WPA (Wi-Fi Protected Access). Seiring

waktu, protokol ini telah mengalami sejumlah evolusi, termasuk WPA dan WPA2. WPA2 telah menjadi standar dalam mengamankan jaringan WiFi selama beberapa tahun terakhir dan telah membantu mengatasi sejumlah masalah keamanan yang ada sebelumnya [2].

Pada tahun 2018, organisasi industri Wi-Fi Alliance merilis protokol keamanan WiFi terbaru, yaitu WPA3, sebagai respons terhadap perubahan lanskap keamanan yang semakin kompleks. WPA3 dirancang dengan tujuan meningkatkan keamanan jaringan WiFi melalui fitur-fitur baru yang lebih kuat, seperti enkripsi yang lebih baik dan perlindungan terhadap serangan brute force [13]. Diharapkan bahwa WPA3 akan memberikan lompatan signifikan dalam melindungi jaringan WiFi dari ancaman keamanan yang semakin canggih. Namun, muncul pertanyaan yang wajar seiring dengan pengenalan WPA3, yakni sejauh mana protokol ini lebih aman dibandingkan dengan pendahulunya, WPA2. Penelitian mengenai perbandingan keamanan antara WPA2 dan WPA3 menjadi sangat penting untuk memahami kemajuan keamanan yang diperkenalkan oleh WPA3 [14].

Untuk mengetahui keamanan keduanya, dapat dilakukan dua pendekatan utama yaitu penetrasi aktif dan pasif. Pendekatan penetrasi aktif melibatkan upaya proaktif untuk mencoba mengeksploitasi potensi kerentanan dalam jaringan. Ini mencakup serangan dan uji penetrasi yang aktif, yang dirancang untuk menguji sejauh mana protokol dapat menahan serangan nyata. Di sisi lain, pendekatan penetrasi pasif lebih bersifat pengawasan dan analisis terhadap lalu lintas jaringan tanpa mengganggu operasionalnya, membantu kita memahami kerentanan yang mungkin ada tanpa tindakan langsung yang merugikan [].

Penelitian ini akan menjawab pertanyaan-pertanyaan penting seputar perbandingan keamanan antara WPA2 dan WPA3 menggunakan kedua pendekatan tersebut, mengidentifikasi kelemahan dan keunggulan dari masing-masing protokol. Selain itu, penelitian ini akan memberikan wawasan berharga kepada

pengguna jaringan WiFi dalam memilih protokol keamanan yang paling sesuai dengan kebutuhan dan tingkat keamanan yang diinginkan.

1.2 Rumusan Masalah

Berdasar latar belakang masalah seperti di 1.1, perumusan masalah dalam penelitian ini adalah:

1. Bagaimana perbandingan keamanan antara protokol WiFi WPA2 dan WPA3 melalui penetrasi aktif?
2. Bagaimana perbandingan keamanan antara protokol WiFi WPA2 dan WPA3 melalui penetrasi pasif?

1.3 Batasan Masalah

Dalam penelitian ini, berikut adalah beberapa batasan masalah:

1. Penelitian ini akan fokus pada penetrasi aktif dan pasif pada jaringan WiFi yang menggunakan protokol WPA2 dan WPA3.
2. Analisis keamanan akan difokuskan pada serangan yang umum terjadi.
3. Penelitian ini tidak akan mempertimbangkan faktor-faktor eksternal seperti konfigurasi jaringan atau tingkat keamanan fisik perangkat jaringan.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah sebagai berikut:

1. Untuk menganalisis perbandingan keamanan antara protokol WiFi WPA2 dan WPA3 melalui pendekatan penetrasi aktif.
2. Untuk menganalisis perbandingan keamanan antara protokol WiFi WPA2 dan WPA3 melalui pendekatan penetrasi pasif.

1.5 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat sebagai berikut:

1. Memberikan pemahaman yang lebih mendalam tentang keamanan protokol WiFi WPA2 dan WPA3.
2. Memberikan panduan bagi pengguna jaringan WiFi dalam memilih protokol keamanan yang sesuai dengan kebutuhan mereka.
3. Menyumbangkan informasi yang relevan dalam pengembangan keamanan jaringan WiFi di masa depan.

1.6 Sistematika Penulisan

Skripsi ini disusun dalam rangka menyajikan hasil penelitian yang dilakukan.

BAB I PENDAHULUAN, Pada bab ini, akan dijelaskan latar belakang penelitian untuk menggambarkan konteks dan alasan pemilihan topik. Penelitian ini berfokus pada analisis perbandingan keamanan protokol WiFi WPA2 dan WPA3 melalui penetrasi aktif dan pasif.

BAB II TINJAUAN PUSTAKA, Pada bagian ini, akan disajikan studi literatur yang mencakup penelitian-penelitian terdahulu terkait dengan analisis keamanan protokol WiFi, WPA2, WPA3, dan pendekatan penetrasi aktif dan pasif. Temuan utama, metodologi, dan hasil dari penelitian-penelitian tersebut akan diberikan.

BAB III METODE PENELITIAN, Pada bagian ini, akan dijelaskan apa yang menjadi fokus penelitian, yaitu analisis perbandingan keamanan protokol WiFi WPA2 dan WPA3 melalui penetrasi aktif dan pasif.

BAB IV HASIL DAN PEMBAHASAN, Bab ini akan membahas hasil dari penelitian yang dilakukan untuk menganalisis perbandingan keamanan protokol WiFi WPA2 dan WPA3 melalui pendekatan penetrasi aktif dan pasif.

BAB V PENUTUP, Bab ini akan merangkum temuan utama dari penelitian ini dan memberikan saran-saran yang relevan.

REFERENSI, mencakup berbagai sumber yang digunakan, seperti buku, jurnal, artikel, dan sumber elektronik.

