BAB I
PENDAHULUAN

1.1 Latar Belakang

Jaringan *Wireless Fidelity* (Wi-Fi) merupakan infrastruktur penting dalam menunjang aktivitas digital masyarakat. Berdasarkan Survei Penetrasi Internet Indonesia 2024 oleh APJII, sekitar 22,38% atau sekitar 49 juta pengguna internet di Indonesia mengakses internet melalui jaringan Wi-Fi yang terpasang di rumah[1]. Namun, seiring meningkatnya penggunaan, aspek keamanan jaringan Wi-Fi masih sering diabaikan. Protokol WPA2 yang banyak digunakan saat ini belum sepenuhnya aman, karena masih memiliki sejumlah celah yang rentan dieksploitasi melalui serangan *brute force* dan *packet sniffing*[2].

Serangan *brute force* dilakukan dengan mencoba berbagai kombinasi karakter secara sistematis hingga menemukan kata sandi yang benar, terutama jika kata sandi tersebut lemah atau mudah ditebak. Sementara itu, serangan *packet sniffing* memungkinkan pelaku menyadap lalu lintas data dalam jaringan dan memperoleh informasi sensitif pengguna, seperti kredensial atau data pribadi[2][3]

Salah satu lingkungan yang rentan terhadap ancaman tersebut adalah tempat tinggal bersama seperti rumah kos. Umumnya, jaringan Wi-Fi di tempat kos hanya dilindungi oleh kata sandi sederhana dan tidak dilengkapi dengan sistem pembatasan akses atau pemantauan aktivitas jaringan. Kondisi ini membuka peluang besar terjadinya penyusupan oleh pengguna internal maupun pihak luar yang memperoleh akses secara tidak sah[3].

Penelitian ini dilakukan untuk menguji dan menganalisis tingkat keamanan jaringan Wi-Fi di Kost 183A yang menggunakan protokol WPA2. Pengujian dilakukan menggunakan metode *penetration testing* melalui simulasi serangan *brute force* dan *packet sniffing* guna mengidentifikasi celah keamanan dan mengevaluasi potensi kebocoran data. Hasil penelitian ini diharapkan dapat memberikan gambaran nyata mengenai tingkat risiko keamanan jaringan Wi-Fi di

lingkungan tempat tinggal bersama, serta menghasilkan rekomendasi mitigasi yang tepat untuk meningkatkan perlindungan jaringan[4].

1.2 Rumusan Masalah

Berdasarkan latar belakang tersebut, rumusan masalah dalam penelitian ini adalah sebagai berikut.

1. Bagaimana efektivitas serangan *brute force* dalam membobol kata sandi pada jaringan Wi-Fi dengan protokol WPA2 di lingkungan kost dan sejauh mana tingkat kerentanan jaringan tersebut terhadap serangan *packet sniffing* dalam memperoleh informasi sensitif?
2. Apa saja celah keamanan yang ditemukan berdasarkan hasil *penetration testing* pada jaringan Wi-Fi pada jaringan tersebut?
3. Bagaimana rekomendasi peningkatan keamanan yang dapat diberikan untuk mitigasi serangan *brute force* dan *packet sniffing* pada jaringan Wi-Fi WPA2?

1.3 Tujuan Penelitian

Tujuan utama dari penelitian ini adalah sebagai berikut.

1. Menganalisis efektivitas serangan *brute force* dalam membobol kata sandi jaringan Wi-Fi WPA2 pada lingkungan kos dan menilai kerentanan jaringan Wi-Fi kos terhadap serangan *packet sniffing* dalam menangkap dan membaca lalu lintas data.
2. Mengidentifikasi celah keamanan yang ditemukan melalui simulasi penetration testing pada jaringan Wi-Fi kos.
3. Memberikan rekomendasi teknis untuk meningkatkan keamanan jaringan Wi-Fi berbasis WPA2 agar lebih tahan terhadap serangan *brute force* dan *sniffing*.

1.4 Manfaat Penelitian

Penelitian ini diharapkan memberikan manfaat sebagai berikut.

1. Memperdalam pemahaman dan keahlian dalam bidang keamanan jaringan, khususnya *penetration testing* pada jaringan WiFi.
2. Dapat menjadi referensi dan dasar bagi penelitian selanjutnya mengenai keamanan jaringan nirkabel.
3. Meningkatkan kesadaran akan pentingnya keamanan jaringan WiFi dan cara-cara untuk melindunginya dari serangan siber.
4. Memberikan masukan berharga dalam meningkatkan kebijakan dan implementasi keamanan jaringan WiFi yang lebih baik.

1.5 Batasan Masalah

Untuk memfokuskan penelitian, batasan masalah dalam penelitian ini adalah sebagai berikut.

1. Objek penelitian adalah jaringan WiFi lokal yang menggunakan protokol keamanan WPA2 Personal (PSK).
2. Serangan yang disimulasikan terbatas pada serangan *brute-force* terhadap otentikasi WiFi dan serangan *sniffing* terhadap lalu lintas data yang tidak terenkripsi atau terenkripsi namun dapat dipecah.
3. Metode yang digunakan adalah *penetration testing* dengan ketersediaan akses dan izin.
4. Alat (*tools*) yang digunakan dalam *penetration testing* adalah alat-alat yang umum digunakan dalam keamanan jaringan Aircrack-ng suite, Wireshark.

5. Analisis difokuskan pada identifikasi kerentanan dan potensi dampak serangan, bukan pada perbaikan *hardware* atau *firmware* perangkat jaringan secara mendalam.

1.6 Sistematika Penulisan

BAB I PENDAHULUAN

Pada bab ini, berisi latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Pada bab ini, membahas teori-teori yang relevan dengan penelitian ini, seperti dasar-dasar teori yang digunakan untuk brute force dan sniffing

BAB III METODE PENELITIAN

Pada bab ini, menjelaskan metode penelitian yang didalamnya terdapat tinjauan umum tentang objek penelitian, analisis masalah, solusi yang ditawarkan, perencanaan.

BAB IV HASIL DAN PEMBAHASAN

bab ini merupakan tahapan yang penulis lakukan dalam melakukan penyerangan dengan teknik *brute force* dan *packet sniffing*.

BAB V PENUTUP

berisi kesimpulan dan saran yang dapat peneliti rangkum selama proses penelitian