BAB 1 PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi dan komunikasi yang pesat telah memengaruhi hampir seluruh aspek kehidupan, dengan salah satu dampak paling signifikan adalah meluasnya penggunaan jaringan nirkabel (Wi-Fi). Teknologi Wi-Fi telah menjadi tulang punggung konektivitas internet di berbagai lingkungan, mulai dari rumah pribadi, perkantoran, hingga fasilitas umum, karena kemudahan akses yang ditawarkannya. Tingginya tingkat adopsi ini tercermin dari jumlah pengguna internet di Indonesia yang telah mencapai sekitar 200 juta jiwa, atau setara dengan ±65% dari total populasi, yang sebagian besar mengandalkan Wi-Fi untuk aktivitas daring mereka (Shiddiqi et al., 2020).

Meskipun memberikan kemudahan, popularitas Wi-Fi menjadikannya target utama bagi para peretas. Sifatnya yang terbuka membuat jaringan nirkabel rentan terhadap berbagai ancaman keamanan yang semakin kompleks, seperti penyadapan (eavesdropping), serangan man-in-the-middle, dan denial of service (DoS). Kelemahan dalam sistem keamanan dapat dieksploitasi untuk mencuri data sensitif, menyalahgunakan akses internet, menyebarkan malware, hingga mengakibatkan kerugian finansial yang signifikan. Oleh karena itu, menjaga kerahasiaan, integritas, dan ketersediaan data pada jaringan Wi-Fi merupakan isu krusial yang menuntut perhatian serius dari setiap pengguna.

Di antara berbagai teknik serangan, dictionary attack merupakan salah satu metode yang paling umum dan efektif digunakan oleh penyerang untuk mendapatkan akses tidak sah ke jaringan Wi-Fi yang dilindungi kata sandi. Serangan ini bekerja dengan cara menebak kata sandi secara sistematis menggunakan daftar kata (wordlist) yang telah dikompilasi dari berbagai sumber, termasuk kata-kata dari kamus bahasa, kombinasi umum, serta data dari kebocoran kata sandi sebelumnya (*Encyclopedia of Cryptography, Security and Privacy, 3rd (Sushil Jajodia, Pierangela Samarati, Moti Yung Etc.)*, n.d.). Efektivitas serangan ini berakar pada kecenderungan manusia untuk menggunakan kata sandi yang lemah, pendek, dan mudah ditebak, sehingga memberikan celah keamanan yang dapat dieksploitasi dengan cepat.

Keberhasilan dan kecepatan sebuah dictionary attack sangat dipengaruhi oleh beberapa faktor kunci yang dapat dievaluasi secara kuantitatif. Faktor utama adalah kekuatan kata sandi itu sendiri, yang ditentukan oleh panjang dan kompleksitas (variasi kombinasi huruf besar, huruf kecil, angka, dan simbol). Selain itu, faktor krusial lainnya adalah kekuatan komputasi yang dimiliki penyerang. Kemajuan teknologi, terutama penggunaan *Graphics Processing Uni*t (GPU) untuk pemrosesan paralel, telah terbukti mampu mempercepat proses peretasan kata sandi secara masif dibandingkan dengan penggunaan CPU konvensional (Alkhwaja et al., 2023).

Meskipun penelitian mengenai keamanan Wi-Fi telah banyak dilakukan, masih terdapat kebutuhan untuk evaluasi yang lebih spesifik mengenai hubungan terukur antara karakteristik "kata sandi umum" dengan "kebutuhan waktu serangan" yang realistis. Oleh karena itu, penelitian ini bertujuan untuk mengevaluasi secara empiris bagaimana variasi panjang dan kombinasi karakter pada kata sandi umum memengaruhi durasi serangan *dictionary attack* yang dilancarkan menggunakan perangkat keras kelas konsumen. Dengan memahami faktor-faktor yang memengaruhi kecepatan serangan secara mendalam, penelitian ini diharapkan dapat memberikan rekomendasi keamanan yang praktis dan dapat diimplementasikan oleh pengguna untuk melindungi jaringan Wi-Fi mereka secara lebih efektif dari ancaman siber yang terus berkembang.

1.2 Rumusan Masalah

Rumusan masalah dari kegiatan ini adalah sebagai berikut:

1. Bagaimana pengaruh langsung dari panjang dan variasi kombinasi karakter (misalnya, hanya angka, hanya huruf, atau kombinasi lengkap) pada "kata sandi umum" terhadap waktu yang dibutuhkan untuk berhasil diretas menggunakan teknik dictionary attack pada jaringan Wi-Fi berenkripsi WPA2-PSK?
2. Seberapa besar peran dan efektivitas dari wordlist (kamus kata sandi) yang berisi puluhan juta kata sandi umum (seperti dari koleksi SecLists) dalam

menentukan tingkat keberhasilan dan kecepatan serangan terhadap jaringan Wi-Fi target?

3. Berdasarkan hasil kuantitatif dari evaluasi waktu serangan, apa saja rekomendasi keamanan yang paling praktis dan langkah-langkah mitigasi yang paling efektif untuk diimplementasikan oleh pengguna umum guna melindungi jaringan Wi-Fi mereka dari ancaman dictionary attack?

1.3 Tujuan

Adapun tujuan dari kegiatan ini adalah sebagai berikut :

1. Menganalisis dan mengukur pengaruh langsung dari panjang serta variasi kombinasi karakter (misalnya, hanya angka, hanya huruf, atau kombinasi lengkap) pada "kata sandi umum" terhadap waktu yang dibutuhkan untuk berhasil meretas jaringan Wi-Fi berenkripsi WPA2-PSK menggunakan teknik *dictionary attack*.
2. Mengevaluasi peran dan efektivitas dari *wordlist* (kamus kata sandi) yang berisi puluhan juta kata sandi umum (seperti dari koleksi SecLists) dalam menentukan tingkat keberhasilan dan kecepatan serangan terhadap jaringan Wi-Fi target.
3. Merumuskan rekomendasi keamanan dan langkah-langkah mitigasi yang praktis serta efektif bagi pengguna umum untuk melindungi jaringan Wi-Fi mereka dari ancaman *dictionary attack*, berdasarkan data kuantitatif yang diperoleh dari hasil evaluasi serangan.

1.4 Manfaat

Penelitian ini diharapkan dapat memberikan manfaat yang signifikan, baik secara praktis bagi para pemangku kepentingan maupun secara akademis bagi pengembangan ilmu pengetahuan.

1. Bagi Pemilik dan Administrator Jaringan Wi-Fi: Memberikan data kuantitatif dan bukti empiris mengenai hubungan langsung antara panjang, kompleksitas karakter, dan jenis wordlist dengan waktu yang dibutuhkan untuk meretas

kata sandi. Hasil analisis ini dapat menjadi dasar dalam pengambilan keputusan untuk menerapkan kebijakan keamanan yang lebih kuat, efektif, dan terukur guna melindungi aset informasi dan infrastruktur jaringan dari akses tidak sah.

2. Bagi Pengguna Wi-Fi Umum dan Masyarakat Luas: Meningkatkan kesadaran (awareness) dan literasi digital mengenai risiko nyata dari penggunaan kata sandi yang lemah dan umum. Hasil penelitian ini dapat berfungsi sebagai materi edukasi yang mudah dipahami, yang menunjukkan secara konkret betapa cepatnya sebuah kata sandi dapat diretas, sehingga mendorong praktik keamanan siber yang lebih baik dalam kehidupan sehari-hari.
3. Bagi Politeknik Negeri Jember: Menjadi dokumen akademik yang dapat memperkaya referensi di perpustakaan, khususnya bagi mahasiswa dan dosen di Jurusan Teknologi Informasi, Program Studi Teknik Komputer. Penelitian ini juga merupakan wujud implementasi Tri Dharma Perguruan Tinggi dalam memberikan kontribusi pemikiran dan analisis praktis terhadap isu keamanan siber yang relevan dengan perkembangan teknologi saat ini.
4. Bagi Peneliti Selanjutnya: Dapat menjadi landasan, data awal, dan sumber rujukan yang valid bagi penelitian-penelitian di masa depan yang ingin mendalami topik keamanan siber. Secara spesifik, penelitian ini dapat menjadi titik awal untuk evaluasi kinerja serangan pada perangkat keras kelas konsumen yang berbeda, pengembangan strategi *wordlist* yang lebih canggih, atau analisis komparatif dengan protokol keamanan yang lebih baru seperti WPA