RINGKASAN

Evaluasi Keamanan Wi-Fi Berdasarkan Kebutuhan Waktu Serangan Terhadap Password Umum Menggunakan Teknik Dictionary Attack, Krishtian Benaya Chandra, NIM E32202368, Tahun 2026, Teknologi Informasi, Politeknik Negeri Jember, I Gede Wiryawan, S.Kom., M.Kom. (Pembimbing).

Keamanan jaringan nirkabel (Wi-Fi) merupakan isu krusial yang menuntut perhatian serius di era digital saat ini. Meskipun protokol WPA2-PSK telah menjadi standar keamanan yang paling banyak digunakan, kekuatan proteksinya sangat bergantung pada kualitas kata sandi yang dipilih oleh pengguna. Di antara berbagai teknik serangan, *dictionary attack* merupakan salah satu metode paling umum dan efektif untuk mendapatkan akses tidak sah ke jaringan Wi-Fi yang dilindungi kata sandi lemah.

Penelitian ini bertujuan untuk menganalisis dan mengukur pengaruh langsung dari panjang serta variasi kombinasi karakter pada kata sandi umum terhadap waktu yang dibutuhkan untuk berhasil meretas jaringan Wi-Fi berenkripsi WPA2-PSK menggunakan teknik *dictionary attack*, mengevaluasi peran dan efektivitas dari *wordlist* yang berisi puluhan juta kata sandi umum dari koleksi SecLists, serta merumuskan rekomendasi keamanan praktis bagi pengguna umum.

Evaluasi dilaksanakan terhadap tujuh target jaringan Wi-Fi dalam lingkungan nyata dengan melakukan simulasi serangan menggunakan perangkat *Wifite* untuk fase penangkapan *handshake/PMKID* dan *Hashcat* untuk fase *cracking* offline pada sistem operasi Kali GNU/Linux Rolling, dengan GPU NVIDIA GeForce MX150 sebagai akselerator komputasi.

Hasil penelitian menunjukkan bahwa kata sandi sederhana seperti deretan angka berurutan (1234567890), pola tanggal lahir (19111991, 01021992), atau kata tunggal berbasis bahasa lokal (bismillah) dapat di-*crack* secara offline dalam waktu 1,0 hingga 17,0 detik. Pengujian pada target dengan protokol WPA3-SAE membuktikan keamanan yang sangat tinggi karena fitur *Protected Management Frames* (PMF) berhasil menggagalkan serangan deautentikasi aktif secara total. Selain itu, eksploitasi WPS *Pixie-Dust* pada target dengan fitur WPS aktif berhasil memperoleh PIN dan kata sandi WPA2 asli dalam waktu 4 menit 55 detik tanpa perlu *dictionary attack* offline. Penggunaan GPU memberikan akselerasi pemrosesan hingga ~8,82 kali lipat (~60.000 H/s) dibandingkan CPU (~6.800 H/s). Penelitian ini merekomendasikan penonaktifan fitur WPS, penggunaan *passphrase* panjang minimal 16 karakter, dan migrasi ke protokol WPA3-SAE untuk meningkatkan keamanan jaringan Wi-Fi.