

ABSTRAK

Ketahanan kata sandi perlu dievaluasi dengan mempertimbangkan panjang dan kompleksitas karakter, algoritma *hashing*, metode serangan, cakupan kandidat dalam *wordlist*, serta kemampuan perangkat komputasi. Oleh karena itu, pengujian empiris diperlukan untuk memperoleh gambaran ketahanan kata sandi pada berbagai skenario serangan. Penelitian ini bertujuan menganalisis pengaruh panjang dan kompleksitas karakter terhadap *time-to-crack*, membandingkan karakteristik keberhasilan *brute force attack* dan *dictionary attack*, serta mengevaluasi pengaruh lingkungan CPU dan GPU terhadap performa pengujian. Penelitian menggunakan eksperimen terapan dengan pendekatan kuantitatif melalui pengujian *offline* menggunakan Hashcat. Data uji terdiri atas 120 kata sandi sintesis dengan enam variasi panjang, empat kategori kompleksitas, dan lima sampel pada setiap kombinasi. Nilai hash dihasilkan menggunakan MD5, SHA-256, dan bcrypt *cost* 10. Pengujian dilakukan pada CPU dan GPU menggunakan *brute force attack* serta *dictionary attack* dengan RockYou dan *wordlist* lokal berbahasa Indonesia. Batas observasi ditetapkan 120 detik per skenario, sedangkan analisis menggunakan *time-to-crack*, *success rate*, *restricted mean survival time* (RMST), dan *throughput*. Hasil menunjukkan bahwa peningkatan panjang dan kompleksitas pada *brute force attack* diikuti penurunan *success rate* dan peningkatan RMST. RockYou menemukan empat target yang tercakup pada MD5 dan SHA-256, sedangkan *wordlist* lokal tidak menemukan target karena tidak ada sampel yang tercakup dalam daftar kandidat. Seluruh target bcrypt belum berhasil ditemukan dalam batas observasi. Pada pengujian *benchmark*, GPU menghasilkan *throughput* 1,72–2,87 kali lebih tinggi daripada CPU, tetapi peningkatan kemampuan komputasi tidak selalu mengubah status keberhasilan pengujian.

Kata kunci: kata sandi, *brute force attack*, *dictionary attack*, RMST, Hashcat.

ABSTRACT

Password resilience should be evaluated by considering password length and character complexity, hashing algorithms, attack methods, wordlist candidate coverage, and computational capability. Therefore, empirical testing is required to describe password resilience under different attack scenarios. This study aims to analyze the effect of password length and character complexity on time-to-crack, compare the success characteristics of brute-force attack and dictionary attack, and evaluate the effect of CPU and GPU environments on testing performance. The study employed an applied experimental method with a quantitative approach through offline testing using Hashcat. The test data consisted of 120 synthetic passwords with six length variations, four complexity categories, and five samples for each combination. Hash values were generated using MD5, SHA-256, and bcrypt with cost 10. Testing was conducted on CPU and GPU environments using brute-force attack and dictionary attack with RockYou and a locally curated Indonesian wordlist. The observation limit was 120 seconds per scenario, while the analysis used time-to-crack, success rate, restricted mean survival time (RMST), and throughput. The results show that increasing password length and complexity in brute-force scenarios was followed by a lower success rate and higher RMST. RockYou recovered four covered targets on MD5 and SHA-256, whereas the local wordlist recovered none because no research samples were included in its candidate list. No bcrypt target was recovered within the observation limit. In benchmark testing, GPU throughput was 1.72–2.87 times higher than CPU throughput, but greater computational capability did not always change recovery status.

Keywords: password, brute-force attack, dictionary attack, RMST, Hashcat.