ABSTRAK

Perkembangan teknologi Internet of Things (IoT) telah memberikan dampak signifikan terhadap meningkatnya jumlah perangkat yang saling terhubung secara otomatis. Salah satu protokol komunikasi yang banyak digunakan dalam lingkungan IoT adalah Message Queuing Telemetry Transport (MQTT), yang dirancang ringan dan efisien. Namun, di balik efisiensinya, MQTT memiliki sejumlah kerentanan terhadap serangan siber seperti brute force, Man-in-the-Middle (MITM), dan Denial of Service (DoS). Minimnya praktik pengujian keamanan (penetration testing) terhadap protokol ini pada tahap awal pengembangan perangkat IoT menjadi permasalahan utama yang diangkat dalam penelitian ini.

Penelitian ini menawarkan solusi berupa prototype pengembangan perangkat lunak *penetration testing* berbasis Python yang dirancang khusus untuk menguji keamanan protokol MQTT. Perangkat lunak ini dilengkapi dengan berbagai fitur seperti pemindaian perangkat MQTT di jaringan, pengujian autentikasi melalui metode *brute force*, simulasi serangan fuzzing, pengukuran *delay* QoS, serta serangan DoS untuk mengidentifikasi potensi kerentanan pada *broker* MQTT. Aplikasi juga disertai dengan tampilan antarmuka grafis berbasis PySide6 serta fitur pencatatan log dan pembuatan laporan pengujian yang terstruktur.

Berdasarkan hasil pengujian black box dan *user acceptance test* (UAT), perangkat lunak berhasil mendeteksi *broker* MQTT aktif, menguji autentikasi, serta mensimulasikan berbagai serangan secara efektif. Aplikasi ini juga terbukti mampu menjalankan skenario serangan yang telah ditetapkan, seperti simulasi *brute force* dan fuzzing dengan stabil. Hasil ini menunjukkan bahwa prototipe perangkat lunak yang dikembangkan dapat digunakan sebagai alat bantu dalam proses pengujian keamanan perangkat IoT berbasis MQTT.

Kata kunci: MQTT, penetration testing, IoT, brute force, fuzzing