ABSTRACT

The development of Internet of Things (IoT) technology has had a significant impact on the increasing number of automatically interconnected devices. One of the most widely used communication protocols in the IoT environment is the Message Queuing Telemetry Transport (MQTT), which is designed to be lightweight and efficient. However, despite its efficiency, MQTT has a number of vulnerabilities to cyberattacks such as brute force, Man-in-the-Middle (MITM), and Denial of Service (DoS). The lack of security testing (penetration testing) practices for this protocol during the initial development phase of IoT devices is the primary problem addressed in this research.

This research offers a solution in the form of a prototype for a Python-based penetration testing software, specifically designed to test the security of the MQTT protocol. The software is equipped with various features, such as scanning for MQTT devices on a network, authentication testing via the brute force method, fuzzing attack simulations, QoS delay measurement, and DoS attacks to identify potential vulnerabilities in the MQTT broker. The application is also furnished with a graphical user interface based on PySide6, as well as logging and structured test report generation features.

Based on the results of black box testing and user acceptance tests (UAT), the software successfully detected active MQTT brokers, tested authentication, and effectively simulated various attacks. The application was also proven to be capable of running designated attack scenarios, such as brute force and fuzzing simulations, with stability. These results indicate that the developed software prototype can be utilized as a supplementary tool in the security testing process for MQTT-based IoT devices.

Keywords: MQTT, penetration testing, IoT, brute force, fuzzing.