ABSTRACT

The rapid adoption of Internet of Things (IoT) devices across various sectors has been accompanied by an increase in cybersecurity risks. Many IoT devices are vulnerable to attacks due to weak configurations, the use of insecure communication protocols, and a lack of pengguna awareness regarding potential threats such as Distributed Denial of Service (DDoS) and Man-in-the-middle (MITM). The limitations of existing security Testing tools, whether in terms of cost, complexity, or protocol coverage, pose a major obstacle for developers and penggunas in identifying and mitigating these vulnerabilities. Therefor e, this research focuses on developing a portable and comprehensive security Testing tool to address this issue.

To tackle this problem, a Prototype penetration Testing device based on the Raspberry Pi 4 was developed, integrating various open-source security Testing tools into a unified system. This solution consists of three main modules: Wifipen for WiFi network Testing, Blue.py for Bluetooth Low Energy (BLE) protocol analysis, and RFIDNFClone for Testing the security of NFC/RFID-based access Cards. The Prototype is designed with a modular and interactive command-line interface (CLI), aiming to provide a portable, affor dable, and pengguna-friendly solution for simulating attacks and identifying security gaps in IoT devices.

The test results demonstrate that this Prototype is highly effective in perfor ming its functions. In WiFi Testing, the system successfully captured a WPA2 handshake in under 30 seconds and cracked the password using a wordlist in less than two minutes. For BLE Testing, the Prototype successfully detected devices, perfor med GATT service enumeration, and wrote data to target Characteristics with a 90% success rate. Meanwhile, in NFC/RFID Testing, the ability to Read UIDs and clone MIFARE Classic Cards showed a success rate of 70-80%. In conclusion, this IoT Pentester Prototype proves to be a reliable and efficient solution for conducting basic security evaluations on the most common wireless communication protocols used in the IoT ecosystem.

Keywords: Internet of Things, Network Security, Penetration Testing, Raspberry Pi, Wireless