ABSTRACT

In today’s rapidly evolving digital landscape, effective network visibility is essential for maintaining security and operational reliability. This work presents a web-based network scanning and vulnerability detection tool developed using Flask, Nmap, and integrated threat intelligence feeds. The system allows users to scan defined IP ranges, identify live hosts, detect open ports, and enumerate running services. It supports both Quick and Deep scan modes, delivering structured and readable outputs. Beyond basic scanning, it correlates vulnerabilities using data from OpenVAS, the Common Weakness Enumeration (CWE) list, and the National Vulnerability Database (NVD). An integrated AI chatbot assists users by providing real-time insights on services, associated risks, and recommended actions. Key features include real-time responses, input validation, a modular architecture, and future extensibility. Planned enhancements involve asynchronous task execution, CVSS-based scoring, and dynamic visualization dashboards. This tool serves as a streamlined platform for students, system administrators, and cybersecurity professionals to perform active network assessments and risk evaluations.

Keywords – enumeration, network scanning, Nmap, Flask, web application, cybersecurity, IP range, real-time feedback, input validation, scalability.