INTISARI

PENGEMBANGAN SISTEM OTOMATIS PEMETAAN KERENTANAN CVE BERDASARKAN HASIL PEMINDAIAN NMAP MENGGUNAKAN PENDEKATAN *RULE-BASED*

Berliana Putri Utami
21/481950/SV/19878

Penelitian ini bertujuan untuk mengembangkan sistem otomatis dalam memetakan kerentanan keamanan berbasis *Common Vulnerabilities and Exposures* (CVE) berdasarkan hasil pemindaian jaringan menggunakan Nmap. Permasalahan utama yang diangkat adalah hasil pemindaian Nmap yang masih berupa data mentah dan belum terhubung secara langsung dengan informasi kerentanan yang relevan, sehingga proses identifikasi masih dilakukan secara manual dan kurang efisien. Penelitian ini menggunakan data hasil pemindaian Nmap sebagai *input* sistem serta data CVE dari sumber resmi sebagai acuan dalam proses pemetaan kerentanan. Pendekatan yang digunakan dalam sistem ini adalah metode *rule-based* yang memanfaatkan pencocokan atribut seperti *service*, *product*, dan *version* untuk menghubungkan hasil pemindaian dengan data CVE. Hasil penelitian menunjukkan bahwa sistem yang dibangun mampu melakukan pemetaan kerentanan secara otomatis dan terstruktur, sehingga dapat meningkatkan efisiensi proses identifikasi kerentanan dibandingkan dengan metode manual. Selain itu, sistem yang dikembangkan juga mampu memberikan hasil yang konsisten berdasarkan aturan yang telah ditetapkan. Dengan demikian, penelitian ini memberikan kontribusi dalam pengembangan sistem otomatis untuk *vulnerability assessment* berbasis hasil pemindaian jaringan, serta menjadi dasar untuk pengembangan lebih lanjut dalam integrasi sistem keamanan siber.

Kata kunci: Nmap, CVE, otomatisasi, keamanan siber, *rule-based*.

ABSTRACT

DEVELOPMENT OF AN AUTOMATED CVE VULNERABILITY MAPPING SYSTTEM BASED ON NMAP SCAN RESULTS USING A RULE-BASED APPROACH

Berliana Putri Utami
21/481950/SV/19878

This study aims to develop an automated system for mapping cybersecurity vulnerabilities based on Nmap network scanning results using the Common Vulnerabilities and Exposures (CVE) framework. The main problem addressed is that Nmap outputs are still in raw form and not directly linked to relevant vulnerability information, making the identification process manual and inefficient. This research utilizes Nmap scan results as system input and CVE data from official sources as references for vulnerability mapping. The approach used in this system is a rule-based method that matches attributes such as service, product, and version to map scan results to relevant CVE data. The results show that the developed system is capable of performing vulnerability mapping automatically and in a structured manner, thereby improving the efficiency of the identification process compared to manual methods. In addition, the system produces consistent results based on predefined rules. This study contributes to the development of automated systems for vulnerability assessment based on network scanning results and provides a foundation for further development in cybersecurity system integration.

Keywords: *Nmap, CVE, automation, cybersecurity, rule-based.*