ABSTRACT

System and network security is important to maintain the integrity, confidentiality, and availability of data in an organization. In this digital age, vulnerability scanning is a key technology for detecting weaknesses in computer systems and networks that can provide opportunities for cyberattacks. However, manual vulnerability scanning methods are often less efficient, especially in environments with many digital devices. One company that is likely to need and also requires a change from this manual system is a company that provides cloud services, which requires ease maintenance of systems, devices, and servers that are used on a fairly large or large scale. This research focuses on the problem of effectiveness and efficiency in detecting and managing security vulnerabilities in information systems. To address this issue, a manual vulnerability scanning approach and an automated approach using OpenSCAP integrated with Ansible are implemented and compared. Experiments were conducted on a total of 3 target computers, and the analysis consisted of comparing the process and time required for both methods to be implemented. The results showed that the use of Ansible automation can affect the process and also the time taken by the vulnerability scanning system where the manual system obtained a total time of 11.98s and for the Ansible automation system, a total time of 12.886s is obtained if a simultaneous scan test is carried out on the three target computer devices. Based on the literature, this longer time can be influenced by the specifications of the hardware used. This study concludes that the automation approach using Ansible and OpenSCAP has a relatively small effect when applied to the use of three devices. There are opportunities for research related to the impact of the hardware specifications used on the duration of the experiment.

Keywords: Vulnerability scanning, Ansible, Time.