ABSTRACT

Automation of network security hardening processes is increasingly important in the face of ever more complex and dynamic cyber threats. This research explores the effectiveness of automation using Ansible compared to manual methods in implementing security hardening on the Linux Ubuntu operating system. The primary focus of this study is to evaluate the time efficiency, consistency, and ease of applying security policies between these two methods. The research methodology involves problem identification, hypothesis formulation, and comparative testing of time between manual and automated methods, accompanied by result analysis. The hardening process was conducted on several virtual machines (VMs) using both Ansible playbooks and manual methods. Manual configuration involved directly applying security settings through the system interface, while automated configuration using Ansible applied security policies simultaneously through playbooks. The research findings indicate that Ansible completes hardening tasks significantly faster, such as firewall configuration, which takes only 10 seconds and 92 milliseconds, compared to the manual method, which takes 1 minute, 38 seconds, and 45 milliseconds. Although the initial setup of Ansible requires 16 minutes and 18.99 seconds, these results confirm that automation with Ansible not only accelerates the overall hardening process but also reduces the risk of human error and ensures consistency in applying security policies, especially on a large scale.

Keywords: Hardening, Automation, Ansible, SSH, Firewall, Time