ABSTRAK

Otomatisasi proses *hardening* keamanan jaringan semakin penting dalam menghadapi ancaman siber yang kian kompleks dan dinamis. Penelitian ini mengeksplorasi efektivitas otomatisasi menggunakan Ansible dibandingkan dengan metode manual dalam penerapan *security hardening* pada sistem operasi Linux Ubuntu. Fokus utama penelitian ini adalah mengevaluasi efisiensi waktu, konsistensi, dan kemudahan penerapan kebijakan keamanan antara kedua metode tersebut. Metode penelitian melibatkan tahapan identifikasi masalah, formulasi hipotesis, serta pengujian perbandingan waktu antara metode manual dan otomatis, disertai analisis hasil. Proses *hardening* dilakukan pada beberapa *virtual machine* (VM) dengan menggunakan Ansible *playbook* dan metode manual. Konfigurasi manual melibatkan penerapan pengaturan keamanan secara langsung melalui antarmuka sistem, sementara konfigurasi otomatis menggunakan Ansible menerapkan kebijakan keamanan secara serentak melalui *playbook*. Hasil penelitian menunjukkan bahwa Ansible menyelesaikan tugas *hardening* secara signifikan lebih cepat, seperti konfigurasi *firewall* yang hanya memakan waktu 10 detik dan 92 milidetik, dibandingkan dengan metode manual yang memakan waktu 1 menit, 38 detik, dan 45 milidetik. Meski setup awal Ansible membutuhkan 16 menit dan 18,99 detik, hasil ini menegaskan bahwa otomatisasi dengan Ansible tidak hanya mempercepat proses *hardening* secara keseluruhan, tetapi juga mengurangi risiko kesalahan manusia dan memastikan konsistensi dalam penerapan kebijakan keamanan, terutama dalam skala besar.

Kata kunci: *Hardening*, Otomasi Ansible, SSH, *Firewall*, Waktu