BAB I PENDAHULUAN

I.1 Latar Belakang

Otomatisasi proses *hardening* jaringan semakin menjadi perhatian utama dalam keamanan siber, didorong oleh kebutuhan untuk memperkuat keamanan secara efisien sekaligus mengurangi potensi kesalahan manusia dan penggunaan sumber daya yang berlebihan. Penelitian terkini menunjukkan bahwa solusi otomatis mampu meningkatkan mekanisme keamanan secara signifikan di berbagai lingkungan jaringan. Sebagai contoh, (Kenfack et al., 2023) mengusulkan otomatisasi mekanisme hardening untuk meningkatkan keamanan jaringan yang diawasi, menunjukkan bagaimana otomatisasi dapat secara efektif mengurangi potensi serangan dan meningkatkan pertahanan jaringan secara keseluruhan. Demikian pula, (Ortiz-Garces et al., 2021) memperkenalkan model yang bertujuan meningkatkan keamanan jaringan kampus melalui penggunaan alat otomatisasi seperti *Ansible*, yang mempermudah penerapan kebijakan keamanan pada berbagai perangkat dan sistem.

Penerapan security hardening secara manual, meskipun efektif, sering kali membutuhkan waktu dan tenaga yang signifikan serta rentan terhadap kesalahan manusia. Otomatisasi, di sisi lain, menawarkan solusi yang lebih efisien, memastikan bahwa langkah-langkah keamanan diterapkan secara merata dan cepat di seluruh sistem. Otomatisasi menggunakan Ansible tidak hanya memungkinkan penerapan hardening secara konsisten, tetapi juga memungkinkan penerapan kebijakan keamanan di lingkungan yang luas tanpa harus mengelola konfigurasi secara manual di setiap perangkat. Hal ini memberikan efisiensi operasional yang penting, terutama ketika mengelola infrastruktur yang besar dan kompleks.

Dalam konteks ini, penelitian ini bertujuan untuk mengeksplorasi dan membandingkan efektivitas serta efisiensi antara metode hardening otomatis menggunakan Ansible dengan metode manual. Eksperimen ini akan dilakukan dalam lingkungan yang terkendali, di mana Ansible digunakan sebagai alat otomatisasi utama untuk menerapkan langkah-langkah keamanan pada virtual machines (VM). Studi ini berfokus pada mengidentifikasi manfaat utama yang

ditawarkan oleh otomatisasi, seperti penghematan waktu dan peningkatan keseluruhan dalam keamanan sistem, dibandingkan dengan pendekatan manual. Otomatisasi melalui Ansible diharapkan dapat memberikan hasil yang lebih konsisten dan efisien dibandingkan metode manual, sekaligus mengurangi potensi kesalahan manusia yang sering kali menjadi faktor utama dalam kegagalan penerapan kebijakan keamanan.

Tidak hanya di ranah penelitian, penerapan otomatisasi menggunakan Ansible juga telah diadopsi oleh berbagai perusahaan besar seperti IBM, Netflix, dan Adobe. Perusahaan-perusahaan ini menggunakan Ansible untuk mengotomatisasi *security hardening* dan manajemen keamanan di lingkungan yang kompleks dan luas, memastikan bahwa kebijakan keamanan diterapkan secara konsisten dan efisien di seluruh infrastruktur mereka. Implementasi Ansible dalam skala besar oleh perusahaan-perusahaan tersebut semakin menegaskan relevansi dan urgensi penelitian ini. Melalui penelitian ini, diharapkan dapat dipahami lebih jauh bagaimana otomatisasi, khususnya dengan Ansible, dapat berkontribusi signifikan dalam peningkatan keamanan sistem dan efisiensi operasional, serta mengatasi tantangan yang dihadapi dalam metode manual.

Tujuan dari eksperimen ini adalah untuk mengevaluasi dampak otomatisasi terhadap kecepatan dan akurasi proses security hardening, serta untuk menilai sejauh mana otomatisasi dapat meningkatkan keamanan sistem dibandingkan dengan metode manual. Hasil dari penelitian ini diharapkan dapat memberikan wawasan yang mendalam mengenai aplikasi praktis dari otomatisasi Ansible dalam upaya hardening keamanan dan potensi pengaruhnya dalam meningkatkan postur keamanan jaringan. Selain itu, penelitian ini dapat menjadi landasan bagi pengembangan lebih lanjut dalam penggunaan otomatisasi untuk keamanan jaringan, membuka jalan bagi penerapan teknologi yang lebih luas di berbagai sektor industri yang membutuhkan keamanan yang handal dan efisien.

I.2 Perumusan Masalah

Dalam konteks keamanan siber dan implementasi S*ecurity Hardening*, beberapa rumusan masalah dapat diajukan:

a. Bagaimana mengelola implementasi keamanan pada server Linux?
b. Bagaimana pengelolaan server Linux dapat dilakukan dengan lebih mudah?
c. Bagaimana cara mengukur tingkat kemudahan dalam pengelolaan server Linux?

I.3 Tujuan Penelitian

Penelitian ini bertujuan untuk:

a. Mengelola keamanan server Linux melalui instalasi perangkat lunak yang mendukung penguatan (hardening) serta menghapus perangkat lunak yang rentan.
b. Mengimplementasikan pengelolaan server secara otomatisasi pada server-server yang memerlukan penguatan keamanan.
c. Melakukan pengukuran kemudahan otomatisasi dibandingkan dengan metode manual berdasarkan waktu yang diperlukan.

I.4 Batasan Penelitian

Batasan-batasan penelitian tugas akhir ini adalah sebagai berikut:

1. Penelitian ini berfokus pada otomasi untuk pengelolaan keamanan pada sistem *OS Linux Ubuntu.*
2. Penelitian ini akan menggunakan pendekatan eksperimental, di mana pengujian dan analisis dilakukan dalam lingkungan yang dikendalikan
3. Penelitian ini tidak membahas aspek *internal system* dari sistem operasi.
4. Penelitian ini berfokus pada perbandingan waktu antara sistem manual dan otomasi.

I.5 Manfaat Penelitian

Hasil penelitian ini diharapkan memberikan kontribusi pada :

1. Teoritis

   Memberikan kontribusi keilmuan terkait pengelolaan *Security Hardening* menggunakan sistem manual dan automasi.

   Mengetahui gambaran tentang hasil perbandingan antara melakukan proses *Security Hardening* yang dilakukan secara manual dengan proses yang dilakukan secara automasi.

2. Teknis

   Memberikan rekomendasi berdasarkan literatur dan hasil uji coba mengenai mekanisme konfigurasi dan implementasi teknis penggunaan software Ansible untuk melakukan Security Hardening yang lebih efektif di masa mendatang.