BAB I PENDAHULUAN

I.1 Latar Belakang

Dalam keamanan sistem informasi, kemampuan untuk mendeteksi dan mengatasi sebuah *vulnerability* sangatlah dibutuhkan. Hal ini berguna untuk mengidentifikasi kerentanan pada sistem pertahanan, sehingga organisasi dapat memperbaiki kerentanan tersebut sebelum terjadinya serangan oleh pihak lain (Rizki, 2023). Metode untuk mendeteksi celah keamanan tersebut biasa dikenal sebagai *vulnerability scanning*.

Vulnerability Scannning merupakan sebuah metode atau proses untuk melakukan identifikasi kelemahan atau celah keamanan pada sistem komputer dan jaringan (Rizki, 2023). Hal ini merupakan metode penting yang dilakukan secara teratur agar dapat menjaga keamanan data dari serangan-serangan *cyber*. *Vulnerability scanning* tidak hanya dapat dilakukan dengan satu metode saja, melainkan ada beberapa metode yang dapat dilakukan terutama metode dengan pengecekan secara manual.

Namun dengan berkembangnya kebutuhan digital sekarang, melakukan *vulnerability scanning* dengan cara manual tidaklah efektif terutama jika suatu perusahaan menggunakan perangkat kerja digital yang terhitung banyak. Jika dilakukan *Vulnerability scanning* secara manual kepada perangkat kerja digital yang banyak, maka Perusahaan harus melakukan pengecekan secara satu per satu dari setiap perangkat yang mereka miliki.

Dilihat pada permasalahan diatas, OpenSCAP *(Security Content Automation Protocol)* dapat digunakan dan diaplikasikan untuk mengubah sistem *scanning* yang awalnya dilakukan secara manual, menjadi otomatis. OpenSCAP *(Security Content Automation Protocol)* sendiri merupakan seperangkat alat *open-source* yang digunakan untuk menerapkan dan mematuhi stpenggunar SCAP *(Security Content Automation Protocol)* bersertifikat NIST (National Institute of Standards and Technology).

OpenSCAP *(Security Content Automation Protocol)* juga dapat diintegrasikan dengan Ansible, agar Perusahaan dapat melakukan pengecekan *vulnerability* kepada semua perangkat kerja digital tanpa harus melakukannya satu per satu. Btech (2023) menyatakan bahwa Ansible merupakan sebuah alat open-source untuk pengaturan perangkat lunak, pengelolaan konfigurasi, dan penerapan aplikasi. Alat ini dapat mengotomatisasi kan suatu proses konfigurasi dan pengelolaan *server*, serta penerapan dan pembaruan aplikasi.

Kerentanan pada sistem dapat dieksploitasi oleh pihak yang tidak bertanggung jawab untuk menimbulkan kerusakan atau mencuri data sensitif. Oleh karena itu, sangat penting untuk menerapkan metode yang efektif untuk mengidentifikasi dan mengelola kerentanan. Salah satu metode yang ada adalah melakukan otomasi pada proses *vulnerability scanning* menggunakan program seperti Ansible. Metode otomatisasi ini berpotensi untuk memudahkan proses *vulnerability scanning* pada perangkat dengan skala besar dibandingkan metode manual. Pada penelitian ini digunakan satu perangkat komputer *virtual* sebagai komputer kontroler dan tiga perangkat komputer *virtual* dengan OS dan spesifikasi yang identic sebagai target komputer Penelitian ini berfokus pada analisis perbandingan metode manual dan otomatis dalam konteks proses yang dilalui dan juga waktu yang diperlukan, yang bertujuan untuk mengetahui metode mana yang lebih efektif dalam meningkatkan keamanan sistem.

I.2 Perumusan Masalah

Adapun rumusan masalah yang akan mendasari penelitian ini adalah:

1. Bagaimana implementasi sistem otomasi menggunakan Ansible berpengaruh pada pengelolaan keamanan?
2. Bagaimana implementasi otomasi Ansible dalam pengelolaan sistem keamanan secara otomatis?
3. Bagaimana penggunaan Ansible sebagai alat otomatisasi dapat mempengaruhi waktu respons terhadap kerentanan keamanan dibandingkan dengan metode manual konvensional?

I.3 Tujuan Penelitian

Penelitian ini bertujuan untuk:

a. Melakukan evaluasi efektivitas otomasi menggunakan Ansible dalam pengelolaan keamanan dengan cara melakukan OpenSCAP *vulnerability scanning*.
b. Melakukan perbandingan proses yang dilalui dengan sistem otomasi menggunakan Ansible terhadap uji coba OpenSCAP *vulnerability scanning*.
c. Melakukan pengukuran waktu respons yang diperoleh dengan sistem otomasi menggunakan Ansible terhadap uji coba OpenSCAP *vulnerability scanning*.

I.4 Batasan Penelitian

Batasan-batasan penelitian tugas akhir ini adalah sebagai berikut:

a. Penelitian ini terbatas pada implementasi otomasi OpenSCAP *vulnerability scanning* menggunakan Ansible dalam pemindaian kerentanan keamanan pada sistem.
b. Penelitian ini akan dilakukan menggunakan satu perangkat *virtual* sebagai komputer kontroler dan tiga perangkat *virtual* yang memiliki spesifikasi identik sebagai komputer target untuk uji coba, menggunakan pendekatan eksperimental dengan pembanding langsung antara penggunaan metode sistem manual dan otomasi Ansible.
c. Metodologi penelitian ini mendasarkan diri pada data kuantitatif dari uji kerentanan keamanan yang dihasilkan oleh Ansible.

I.5 Manfaat Penelitian

Manfaat penelitian ini:

1. Teoritis
    - Memberikan kontribusi keilmuan terkait pengelolaan OpenSCAP *vulnerabilty scanning* menggunakan sistem manual dan sistem otomasi.
    - Mengetahui gambaran tentang hasil perbandingan antara melakukan proses OpenSCAP *vulnerability scanning* yang dilakukan secara manual dengan proses yang dilakukan secara otomasi menggunakan Ansible.
2. Teknis
    - Mengetahui cara-cara teknis penggunaan Ansible sebagai alat untuk melakukan otomasi.
    - Memberikan rekomendasi berdasarkan kajian dan hasil uji coba pembanding sistem untuk melakukan OpenSCAP *vulnerability scanning* yang lebih efektif untuk dilakukan kedepannya.