BAB 1
PENDAHULUAN

1.1 Latar Belakang

Keamanan sistem informasi merupakan aspek krusial dalam menjaga stabilitas dan keberlangsungan layanan pada infrastruktur teknologi informasi (TI) organisasi. Di era digital saat ini, ancaman siber semakin meningkat, baik dari segi frekuensi maupun kompleksitasnya. Fenomena ini ditegaskan oleh penelitian Adil & Beeh (2024), yang menggarisbawahi eskalasi serangan siber dengan potensi kerugian finansial yang sangat besar di tingkat global. Serangan seperti ransomware, malware, hingga eksploitasi kerentanan perangkat lunak tidak lagi menyasar hanya perusahaan besar, tetapi juga institusi pendidikan, sektor publik, dan organisasi skala menengah. Studi empiris menunjukkan bahwa sebagian besar pelanggaran keamanan seringkali berasal dari eksploitasi kerentanan pada sistem yang belum diperbarui (Kurniawan & Saputra, 2024), menegaskan bahwa manajemen patch yang efektif adalah kunci pertahanan awal.

Masalah utama yang sering dihadapi organisasi adalah keterlambatan atau kelalaian dalam melakukan pembaruan sistem operasi, khususnya pada infrastruktur on-premise yang masih dikelola secara manual. Dalam praktiknya, proses pembaruan yang dilakukan secara manual membutuhkan waktu, tenaga, dan koordinasi yang tinggi, terutama jika jumlah server yang dikelola cukup banyak. Penelitian oleh Rafsyandjani (2025) secara spesifik mengidentifikasi bahwa proses patching manual pada infrastruktur TI berskala besar seringkali menyebabkan penundaan signifikan, menciptakan celah keamanan yang rentan dieksploitasi. Keterlambatan ini menyebabkan banyak sistem berjalan dengan versi perangkat lunak yang rentan, membuka peluang besar bagi penyerang untuk mengeksploitasi celah keamanan tersebut

Di sisi lain, banyak organisasi juga mulai mengadopsi infrastruktur cloud seperti Google Cloud Platform (GCP) untuk mendapatkan efisiensi dan skalabilitas. Namun, penggunaan cloud tidak serta-merta menghilangkan tanggung jawab pengguna dalam mengelola keamanan, termasuk pembaruan sistem. Pada model Infrastructure as a Service (IaaS), tanggung jawab pengelolaan sistem operasi,

termasuk patching rutin, tetap berada di tangan pengguna (Acheampong et al., 2022). Ketika organisasi menggunakan kombinasi lingkungan on-premise dan cloud (hybrid cloud), tantangannya menjadi semakin besar. Penelitian Afifi Al-Atsari & Suharjo (2023) membahas bagaimana inkonsistensi dalam manajemen keamanan antara kedua lingkungan ini dapat menciptakan titik-titik kerentanan serius, menekankan perlunya pendekatan terpadu.

Untuk mengatasi berbagai tantangan tersebut, otomatisasi manajemen patch menjadi solusi yang semakin relevan dan efektif. Salah satu alat otomasi yang banyak digunakan adalah Ansible, platform open-source yang dikembangkan oleh Red Hat untuk mengotomatisasi provisioning, konfigurasi, dan pembaruan sistem secara terstruktur dan konsisten (Red Hat, 2024). Ansible bekerja dengan pendekatan agentless, memanfaatkan protokol SSH untuk berkomunikasi dengan server target tanpa perlu instalasi agen tambahan, sehingga memudahkan implementasi dan mengurangi kompleksitas pengelolaan. Melalui penggunaan Playbook yang ditulis dalam bahasa deklaratif YAML, Ansible memungkinkan administrator mendefinisikan kondisi akhir yang diinginkan dari sistem, sekaligus menjamin idempotensi agar eksekusi berulang tidak menyebabkan perubahan berlebihan (Ansible Documentation, 2024). Berbagai studi dan kasus nyata telah membuktikan bahwa penerapan Ansible dapat secara signifikan mempercepat proses patching dan konfigurasi sistem, meminimalkan risiko kesalahan manual, serta mendukung pengelolaan infrastruktur TI skala besar secara efisien dan konsisten di lingkungan on-premise maupun cloud (BONbLOC Technologies, 2023).

Berdasarkan permasalahan tersebut, proyek ini dilaksanakan dengan tujuan untuk merancang dan mengimplementasikan solusi otomatisasi pembaruan patch keamanan menggunakan Ansible pada lingkungan hybrid (on-premise dan cloud). Proyek ini diharapkan dapat menjawab permasalahan keterlambatan pembaruan, meminimalisir risiko keamanan akibat sistem yang tidak up-to-date, serta meningkatkan efisiensi operasional dalam pengelolaan infrastruktur TI. Dengan adanya solusi ini, organisasi dapat menjaga keamanan sistem secara lebih proaktif dan konsisten, tanpa membebani sumber daya manusia secara berlebihan.

1.2 Perumusan Masalah

Berdasarkan latar belakang di atas, rumusan masalah dalam penelitian ini adalah:

1) Bagaimana cara menerapkan Ansible untuk mengotomatisasi pembaruan *security patch* pada infrastruktur *on-premise* dan *cloud* ?
2) Sejauh mana efektivitas otomatisasi menggunakan Ansible dalam mempercepat dan mengamankan proses pembaruan sistem ?
3) Apa saja tantangan yang dihadapi dalam menerapkan otomatisasi pengelolaan sistem keamanan menggunakan Ansible ?

1.3 Batasan Masalah

Agar penelitian lebih fokus dan terarah, penelitian ini memiliki beberapa batasan, yaitu:

1) Penelitian ini hanya berfokus pada penggunaan Ansible untuk mengelola dan memperbarui sistem keamanan pada sistem operasi berbasis Linux seperti Ubuntu.
2) Infrastruktur yang digunakan meliputi infrastruktur *on-premise* serta infrastruktur berbasis *cloud* menggunakan *Google Cloud Platform* (*GCP*).
3) Pengujian efektivitas dilakukan berdasarkan tiga parameter utama, yaitu waktu implementasi pembaruan, akurasi dalam penerapan patch, dan dampak terhadap performa sistem.
4) Penelitian ini tidak mencakup aspek keamanan fisik dari infrastruktur TI.

1.4 Tujuan dan Manfaat

1.4.1 Tujuan

Adapun tujuan dari penelitian ini adalah merancang dan mengembangkan sistem otomatisasi menggunakan Ansible untuk pengelolaan sistem keamanan pada infrastruktur *on-premise* dan *cloud*.

1.4.2 Manfaat

Hasil dari penelitian ini diharapkan dapat memberikan manfaat sebagai berikut:

1) Menghasilkan sistem otomatisasi pembaruan *patch* keamanan yang mampu menerapkan pembaruan secara serentak pada beberapa *server* berbasis *on-premise* dan *cloud* menggunakan Ansible.
2) Meningkatkan konsistensi penerapan *patch* keamanan pada seluruh *managed node* sehingga setiap *server* memperoleh pembaruan sesuai *playbook* yang telah ditentukan.
3) Menjadi referensi bagi organisasi yang ingin mengimplementasikan otomatisasi dalam pengelolaan sistem keamanan untuk mendukung infrastruktur TI *hybrid* mereka.