BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Kemajuan teknologi informasi yang pesat telah mendorong peningkatan yang signifikan dalam pemanfaatan jaringan komputer di berbagai bidang. Router menjadi komponen utama jaringan yang memfasilitasi koneksi dan komunikasi antar perangkat. Router Mikrotik khususnya telah menjadi populer karena fiturnya yang memadai dan harganya yang terjangkau, terutama untuk penggunaan jaringan skala kecil hingga menengah (Muhammad Wildan Putra Pratama et al., 2024a). Seiring meningkatnya ketergantungan terhadap infrastruktur jaringan, tantangan dalam menjaga keamanan perangkat jaringan semakin kompleks. Router, sebagai gerbang utama lalu lintas data, menjadi salah satu target serangan siber (Prasetyo et al., 2024). Salah satu jenis serangan yang sering terjadi adalah serangan *brute force*, yaitu serangan yang digunakan untuk menebak kombinasi username dan password hingga mendapatkan akses tidak sah ke perangkat sistem.

Serangan *brute force* yang menargetkan protokol penting seperti FTP (File Transfer *Protocol*) dan SSH (Secure Shell) berpotensi membuka celah besar dalam sistem keamanan jaringan. Protokol-protokol ini umum digunakan dalam pengelolaan perangkat jaringan, dan ketika disusupi, dapat memungkinkan penyerang untuk mengakses dan mengendalikan perangkat sistem. Oleh karena itu, peningkatan keamanan pada protokol FTP dan SSH, khususnya pada perangkat seperti router MikroTik, menjadi langkah penting dalam upaya memitigasi ancaman tersebut (Fauzi et al., 2024a).

Port Blocking dan *Port Knocking* hadir sebagai strategi keamanan yang dapat digunakan untuk mengatasi permasalahan tersebut (Putri ayu agita & Soim, 2023). *Port Blocking* bekerja dengan menutup akses port secara *default*, sementara *Port Knocking* memungkinkan akses hanya setelah urutan "*Knocking*" (koneksi) khusus pada beberapa port tertentu. Kombinasi kedua metode ini menciptakan lapisan keamanan tambahan yang dapat mengurangi ancaman serangan, karena port-port penting seperti SSH dan FTP menjadi "tertutup" bagi penyerang.

Namun, penerapan *Port Blocking* dan *Port Knocking* secara manual pada perangkat MikroTik memiliki kelemahan, yang dimana proses konfigurasi manual yang dilakukan rentan terhadap kesalahan manusia yang dapat menyebabkan celah keamanan atau gangguan layanan jaringan. Tantangan serupa akibat ketergantungan pada konfigurasi manual jaringan juga didokumentasikan oleh Yogantara et al. (2025), yang menemukan bahwa proses pengelolaan manual pada layanan RT/RW Net tidak hanya menyebabkan lamanya waktu operasional, tetapi juga berpotensi menimbulkan kerugian finansial dan penurunan kualitas layanan. Temuan tersebut semakin menegaskan urgensi pengembangan solusi otomatisasi yang mampu menggantikan proses manual dalam melakukan konfigurasi perangkat jaringan.

Kesalahan konfigurasi keamanan dapat menimbulkan dampak serius apabila pengaturan tidak ditetapkan dan diterapkan dengan benar. Nilai konfigurasi *default* yang tidak diubah sering kali menjadi celah yang dapat dieksploitasi oleh pelaku kejahatan siber (Loureiro, 2021). Hal ini dibuktikan secara langsung dalam lingkungan nyata oleh Listartha & Saskara (2024), yang dalam pengujian keamanan jaringan WiFi Universitas Pendidikan Ganesha menggunakan metode Penetration

Testing Execution Standard (PTES) menemukan sejumlah perangkat jaringan aktif yang masih menggunakan kredensial *default* dari pabrik. Kondisi ini memungkinkan akses tidak sah yang berpotensi menimbulkan pencurian data, manipulasi konfigurasi, hingga penggunaan sumber daya jaringan secara ilegal. Oleh karena itu, pengembangan alat bantu untuk otomatisasi konfigurasi sangat direkomendasikan agar proses pengaturan dan pengamanan sistem menjadi lebih sederhana, terutama bagi administrator jaringan dengan tingkat keahlian yang beragam (Arbi Murad et al., 2025). Hal ini sejalan dengan hasil penelitian Santyadiputra et al. (2021) yang membuktikan bahwa implementasi *network automation* terbukti efektif dalam mengurangi human error dan meningkatkan efisiensi administrasi jaringan secara signifikan.

Dalam konteks otomatisasi konfigurasi perangkat jaringan, terdapat beberapa platform yang tersedia seperti Chef, Puppet, dan Ansible. Namun, untuk otomatisasi jaringan khususnya pada perangkat seperti Mikrotik, Ansible menjadi pilihan yang lebih tepat karena beberapa alasan penting. Pertama, Ansible bersifat *agentless*, yang berarti tidak memerlukan instalasi software tambahan pada perangkat target. Hal ini sangat penting karena perangkat jaringan seperti router Mikrotik memiliki keterbatasan dalam menjalankan agent tambahan dan umumnya hanya menyediakan akses melalui SSH atau API. Kedua, Chef dan Puppet dirancang dengan arsitektur *client-server* yang memerlukan agent pada setiap node yang dikelola, sedangkan perangkat jaringan umumnya tidak mendukung instalasi agent tersebut. Ketiga, Ansible menggunakan protokol SSH yang sudah tersedia secara native pada sebagian besar perangkat jaringan, sehingga tidak memerlukan konfigurasi tambahan yang kompleks.

Ansible, sebagai platform otomatisasi, menawarkan solusi untuk mengatasi tantangan tersebut. Kemampuannya dalam mengelola konfigurasi secara terpusat dapat meminimalkan risiko kesalahan manusia dan mempercepat waktu implementasi, sehingga memastikan konsistensi konfigurasi pada semua perangkat. Berdasarkan penelitian yang dilakukan oleh Singh Chauhan (2025), penerapan otomatisasi mampu mengurangi waktu yang dibutuhkan untuk perubahan konfigurasi keamanan hingga 81,25%, serta meningkatkan akurasi konfigurasi sebesar 23%.

Meskipun demikian, implementasi Ansible untuk otomatisasi konfigurasi keamanan Mikrotik yang meliputi *Port Blocking* dan *Port Knocking* belum banyak dikembangkan. Sebagian besar penelitian hanya berfokus pada konteks otomatisasi konfigurasi dasar dengan pola *Port Knocking* yang bersifat statis. Pendekatan statis ini memiliki keterbatasan karena urutan port yang tetap berpotensi dipelajari dan dieksploitasi oleh penyerang. Sebaliknya, penerapan *Port Knocking* dinamis memiliki kelebihan signifikan karena mampu mengubah urutan port secara otomatis berdasarkan aktivitas dan deteksi pola serangan, seperti *brute force* pada layanan FTP dan SSH. Mekanisme ini membuat sistem keamanan menjadi lebih dinamis, sulit diprediksi, serta mampu merespons ancaman tanpa memerlukan intervensi manual administrator. Oleh karena itu, terdapat kesenjangan signifikan dalam pengembangan sistem yang dapat secara adaptif mendukung respons terhadap ancaman keamanan pada perangkat Mikrotik.

Kebutuhan akan sistem keamanan adaptif menjadi semakin penting di tengah kondisi ancaman keamanan jaringan yang terus berkembang. Sistem semacam ini idealnya memiliki kemampuan untuk menganalisis aktivitas dan mengenali pola-

pola mencurigakan, serta secara otomatis menyesuaikan konfigurasi keamanan guna merespons potensi ancaman. Namun, tingkat implementasi sistem keamanan adaptif masih tergolong rendah. Berdasarkan laporan Cybersecurity Insiders tahun 2024, hanya sekitar 25% organisasi yang telah menerapkan solusi Cloud-Native Application Protection Platform (CNAPP) secara menyeluruh dalam infrastruktur mereka. Hal ini menunjukkan adanya kesenjangan yang signifikan antara pengakuan terhadap pentingnya adaptasi otomatis dalam sistem keamanan jaringan dan realisasi penerapannya di lapangan.

Berdasarkan permasalahan tersebut, penelitian ini dirancang untuk menjawab kesenjangan yang ada dengan mengembangkan solusi otomatisasi berbasis Ansible yang tidak hanya dapat melakukan konfigurasi *Port Blocking* dan *Port Knocking* Dinamis pada perangkat Mikrotik, tetapi juga mampu merespons secara adaptif terhadap ancaman yang terdeteksi. Melalui analisis akses terhadap port FTP dan SSH, sistem yang dibangun akan mampu mengubah urutan *Port Knocking* secara otomatis, sehingga menciptakan mekanisme pertahanan yang dinamis dan sulit diprediksi oleh pihak yang berniat jahat.

1.2 Identifikasi Masalah

Berdasarkan latar belakang yang telah dipaparkan, maka dapat diidentifikasi beberapa permasalahan utama sebagai berikut:

1. Konfigurasi keamanan *Port Blocking* dan *Port Knocking* pada router Mikrotik masih banyak dilakukan secara manual, yang berisiko menimbulkan kesalahan konfigurasi, memakan waktu, serta tidak efisien dalam implementasi pada jaringan yang menggunakan perangkat router Mikrotik berskala kecil hingga menengah.

2. Belum banyak dibahas secara khusus solusi otomatisasi konfigurasi berbasis Ansible yang mampu mengintegrasikan *Port Blocking* dan *Port Knocking*, termasuk kemampuan untuk merubah urutan *Port Knocking* berdasarkan deteksi ancaman keamanan.

1.3 Rumusan Masalah

Berdasarkan latar belakang masalah dan identifikasi permasalahan di atas maka permasalahan dapat dirumuskan sebagai berikut:

1. Bagaimana rancangan sistem otomatisasi menggunakan Ansible dan penerapan *event-driven* pada konfigurasi router Mikrotik?
2. Bagaimana skenario pengujian untuk mengevaluasi ketepatan konfigurasi *Port Blocking* dan *Port Knocking* pada router Mikrotik yang dikonfigurasikan menggunakan Ansible?
3. Bagaimana cara mengetahui efisiensi konfigurasi *Port Blocking* dan *Port Knocking* yang dilakukan secara manual dengan yang dilakukan secara otomatis?

1.4 Batasan Masalah

Untuk membatasi penelitian Agar penelitian ini terfokus dan terarah, maka batasan masalah yang ditetapkan adalah sebagai berikut:

1. Penelitian ini terbatas pada penanganan ancaman berupa serangan *brute force* yang ditargetkan pada port FTP dan SSH, dengan fokus hanya pada implementasi pengamanan menggunakan metode *Port Blocking* dan *Port Knocking*.

2. Infrastruktur yang digunakan dalam penelitian ini berbasis simulasi virtualisasi menggunakan GNS3, bukan pada infrastruktur jaringan produksi nyata.

1.5 Tujuan Penelitian

Adapun tujuan yang hendak dicapai dalam penelitian ini adalah sebagai berikut:

1. Mengembangkan sistem otomatisasi berbasis Ansible yang mampu mengimplementasikan konfigurasi *Port Blocking* dan *Port Knocking* pada router Mikrotik, dengan kemampuan deteksi terhadap aktivitas mencurigakan pada akses remote FTP dan SSH, serta melakukan adaptasi otomatis urutan *Port Knocking* berdasarkan *event-driven*.
2. Untuk memvalidasi ketepatan konfigurasi *Port Blocking* dan *Port Knocking* pada router Mikrotik yang dikonfigurasi melalui Ansible, dengan metodologi evaluasi yang mencakup pengujian fungsional.
3. Untuk mengetahui tingkat efisiensi waktu konfigurasi *Port Blocking* dan *Port Knocking* pada router Mikrotik antara metode manual dengan otomatisasi menggunakan Ansible.

1.6 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat, diantaranya adalah sebagai berikut:

1. Memberikan solusi untuk meningkatkan efisiensi dan konsistensi dalam proses konfigurasi *Port Blocking* dan *Port Knocking* pada router Mikrotik melalui otomatisasi Ansible, sehingga meminimalkan kesalahan konfigurasi dan mempercepat konfigurasi keamanan secara serentak.

2. Menyediakan metode deteksi dini terhadap aktivitas mencurigakan di protokol FTP dan SSH, yang mampu secara otomatis memicu penyesuaian konfigurasi keamanan (urutan *Port Knocking*) tanpa intervensi manual.
3. Menjadi referensi praktis bagi administrator jaringan dan profesional TI dalam mengimplementasikan konsep otomatisasi konfigurasi keamanan berbasis Ansible untuk memperkuat sistem pertahanan jaringan, khususnya di lingkungan jaringan skala kecil hingga menengah.