202110370311345
Eureka Diaandisy
Prodi Informatika

BAB I
PENDAHULUAN

1.1 Latar Belakang

Dalam konteks keamanan jaringan, transformasi digital tidak hanya terbatas pada adopsi perangkat lunak dan perangkat keras, tetapi juga mencakup pengelolaan serta perlindungan data dari ancaman siber yang semakin kompleks [1]. Serangan *brute force* merupakan metode serangan yang mencoba kombinasi *login* secara berulang-ulang hingga berhasil menembus sistem [2]. Serangan ini krusial karena dapat menyebabkan kebocoran data, pengambilalihan kontrol perangkat, dan berbagai kerugian operasional pada organisasi yang tidak memiliki perlindungan autentikasi yang memadai [3]. Dalam penelitian Aji dkk. dilaporkan tercatat 259.646 percobaan *brute force* pada server web universitas dalam suatu periode pengamatan [4]. Pada tingkat global, *Data Breach Investigations Report* (DBIR) 2025 menunjukkan *credential abuse* meningkat 34% dibanding tahun sebelumnya [5], menegaskan tren serangan berbasis kata sandi yang semakin marak.

MikroTik RouterOS adalah sistem operasi berbasis Linux yang memungkinkan sebuah komputer difungsikan sebagai perangkat router. Fleksibilitasnya dalam mengelola jaringan kabel dan nirkabel membuatnya banyak diadopsi oleh berbagai pihak, seperti penyedia layanan internet, pengelola hotspot, maupun warnet [6]. Sebagai perangkat jaringan yang populer, MikroTik menjadi salah satu sasaran utama serangan *brute force* melalui protokol SSH. Serangan *brute force* terhadap SSH dapat membuka akses tidak sah, mengakibatkan perubahan konfigurasi, pencurian data, bahkan pengendalian penuh atas jaringan [7].

SSH sendiri adalah protokol berbasis TCP/IP yang menyediakan komunikasi aman melalui enkripsi dan autentikasi yang kuat. SSH menjamin bahwa identitas pengguna dapat diverifikasi secara andal, data yang dikirim tetap rahasia, dan integritas pesan terjaga, sehingga SSH menjadi solusi penting dalam menjaga privasi dan keamanan koneksi jarak jauh antar perangkat di jaringan [8].

Oleh karena itu, penelitian ini mengusulkan penerapan *Multi-Factor Authentication* (MFA) sebagai solusi preventif yang lebih efektif dalam memperkuat keamanan SSH pada MikroTik. MFA mengharuskan pengguna melewati lebih dari satu tahap verifikasi, misalnya *password* dan kode OTP. Pada penelitian ini, MFA diimplementasikan menggunakan OTP melalui RADIUS dan User Manager.

Dalam penelitian ini, digunakan *Time-based One-Time Password* (TOTP) sebagai faktor verifikasi tambahan. TOTP bekerja dengan menghasilkan kode autentikasi sekali-pakai yang dihitung dari *shared secret* dan nilai waktu saat itu [9]. Setiap kode hanya berlaku dalam interval waktu singkat, sehingga kode akan terus berubah secara otomatis. Pada saat proses autentikasi, server menghitung ulang kode berdasarkan waktu dan *shared secret* yang sama untuk memverifikasi kecocokannya. Apabila terdapat perbedaan waktu atau kode yang dimasukkan tidak sesuai, autentikasi akan langsung gagal. Sifat TOTP yang dinamis dan berbatas waktu ini membuatnya tidak dapat diprediksi maupun digunakan kembali, sehingga memberikan perlindungan yang jauh lebih kuat terhadap serangan brute force yang mengandalkan kombinasi statis.

1.2 Rumusan Masalah

Masalah yang akan dikaji dalam penelitian ini dirumuskan berdasarkan latar belakang yang telah diuraikan sebagai berikut:

a. Bagaimana kerentanan layanan SSH pada perangkat MikroTik terhadap serangan *brute force* ketika hanya menggunakan autentikasi satu faktor (*username* dan *password*)?
b. Bagaimana penerapan *Multi-Factor Authentication* (MFA) menggunakan OTP melalui RADIUS dan User Manager pada layanan SSH MikroTik?
c. Sejauh mana efektivitas MFA dalam mencegah serangan *brute force* pada layanan SSH MikroTik?
d. Bagaimana dampak penerapan MFA terhadap performa sistem (CPU *usage* dan *bandwidth*) pada perangkat MikroTik?

1.3 Tujuan Penelitian

Tujuan dari penelitian ini adalah:

a. Menganalisis kerentanan SSH MikroTik terhadap serangan *brute force* pada kondisi tanpa MFA.
b. Menerapkan mekanisme MFA berbasis OTP melalui RADIUS dan User Manager pada SSH MikroTik.
c. Menguji dan mengevaluasi efektivitas MFA dalam mencegah serangan *brute force*.
d. Mengukur dampak penerapan MFA terhadap kinerja perangkat yang ditinjau dari penggunaan CPU dan *bandwidth*.

1.4 Batasan Penelitian

Penelitian ini memiliki batasan sebagai berikut:

a. Pengujian dilakukan dalam lingkungan virtual menggunakan PNETLab, sehingga tidak mencakup variabel kondisi jaringan nyata.
b. Jenis MFA yang digunakan terbatas pada OTP berbasis waktu (TOTP) melalui integrasi RADIUS dan User Manager.
c. Serangan *brute force* diuji menggunakan THC-Hydra dengan konfigurasi *dictionary attack* dan parameter *default*.
d. Fokus penelitian berada pada keamanan autentikasi SSH MikroTik, tidak mencakup layanan lain seperti FTP atau API.
e. Kinerja sistem yang dianalisis hanya meliputi metrik CPU *usage* dan *bandwidth* seperti yang ditetapkan pada parameter evaluasi penelitian.