BAB II
TINJAUAN PUSTAKA

2.1 Penelitian Terdahulu

Penelitian-penelitian terdahulu mengkaji beragam teknik untuk meningkatkan keamanan akses SSH dan jaringan Mikrotik. Beberapa studi menekankan proteksi jaringan melalui filter rules dan IDS/IPS, sementara yang lain meneliti metode otentikasi tambahan. Sebagai contoh, Yefta menemukan bahwa penggunaan port knocking dipadukan dengan *action tarpit* pada Mikrotik efektif meminimalkan penyusupan tidak sah dengan menutup akses port hingga sinyal khusus diterima [10]. Arifwidodo dkk. menganalisis performansi perangkat Mikrotik di bawah serangan brute force dan DDoS menggunakan *honeypot*, dan menunjukkan beban CPU yang meningkat tajam terutama pada skenario DdoS [11]. Usman dkk. membangun sistem Intrusion Prevention System (IPS) untuk mencegah serangan brute force pada layanan SSH Mikrotik [12]. Selain itu, Haeruddin dkk. menguji autentikasi dua-faktor (menggunakan One-Time Password) pada jaringan *Zero Trust*, yang menunjukkan bahwa MFA dapat menambah lapisan keamanan akses SSH [1]. Tabel 2.1 berikut merangkum fokus, metode, dan hasil dari penelitian-penelitian tersebut.

Tabel 2.1 Penelitian Terdahulu

Peneliti (Tahun)	**Fokus Penelitian**	**Metode Keamanan yang Digunakan**	**Hasil Penelitian**
Yefta (2019) [10]	Pengamanan akses SSH menggunakan port knocking dan tarpit di Mikrotik	*Port Knocking*; *Action Tarpit*	Port hanya terbuka setelah urutan knock berhasil, sehingga menurunkan risiko eksploitasi brute force.
Arifwidodo dkk. (2021) [11]	Analisis performansi Mikrotik di bawah serangan Brute Force dan DDoS	*Honeypot*; *Port Forwarding*	DDoS lebih berdampak signifikan terhadap performa CPU dibanding brute force.

Usman dkk. (2024) [12]	Sistem keamanan SSH Mikrotik untuk mencegah brute force dengan IPS	*Intrusion Prevention System* (IPS); Pembatasan IP	IPS berhasil mendeteksi serangan brute force dan memblokir alamat IP pelaku.
Haeruddin dkk. (2024) [1]	Implementasi keamanan jaringan model Zero Trust dengan MFA untuk SSH	Jaringan Virtual (ZeroTier); *Multi-Factor Authentication* (OTP via Google Authenticator)	MFA efektif menolak akses tanpa kode OTP.
Setyowibowo dkk. (2022) [13]	Keamanan jaringan hotspot dengan simple port knocking dan automated backup	Simple Port Knocking; Automasi Backup	Port knocking berhasil menambah keamanan hotspot.
Fauzi dkk. (2024) [14]	Perancangan keamanan Mikrotik terhadap serangan FTP dan SSH brute force	Firewall Rules; Pembatasan Login	Firewall terbukti dapat menahan brute force dasar.
Haeruddin dkk. (2025) [15]	MFA untuk optimasi keamanan akses data di PT. ABC	MFA (Google Authenticator); OTP	MFA meningkatkan keamanan akses internal perusahaan.

Penelitian terdahulu menunjukkan bahwa mayoritas solusi keamanan SSH dan Mikrotik berfokus pada proteksi jaringan, seperti firewall, port knocking, dan IPS. Misalnya, Setyowibowo dkk. menekankan simple port knocking sebagai metode untuk menyembunyikan port layanan [13], sedangkan Fauzi dkk. merancang aturan firewall untuk menahan serangan brute force [14].

Beberapa penelitian mulai mengarah pada autentikasi berlapis, seperti MFA (Haeruddin dkk., 2024; 2025), namun implementasinya belum diarahkan khusus pada SSH Mikrotik.

2.2 Research Gap

Berdasarkan analisis penelitian terdahulu, terdapat sejumlah celah (*gap*) penelitian yang menunjukkan bahwa topik *Multi-Factor Authentication* (MFA) pada SSH Mikrotik belum banyak dieksplorasi. Sebagian besar penelitian berfokus pada firewall,

port knocking, dan Intrusion Prevention System (IPS) yang bekerja di lapisan jaringan. Hanya sedikit penelitian yang meneliti autentikasi berlapis, dan belum ada yang menguji implementasi MFA secara langsung pada SSH Mikrotik. Untuk memperjelas celah penelitian, disusun Tabel 2.2 berikut.

Tabel 2.2 Research Gap

Aspek yang Dibahas	**Studi Terkait**	**Kekurangan / Kebutuhan Lanjutan**
Autentikasi Multi-Faktor (MFA)	Haeruddin dkk. (2024); Haeruddin dkk. (2025)	MFA terbukti menambah keamanan, tetapi tidak diterapkan pada Mikrotik SSH. Perlu penelitian yang menguji MFA berbasis OTP/RADIUS langsung pada MikroTik RouterOS.
Firewall / Filter Rules pada Mikrotik	Fauzi dkk. (2024)	Firewall mampu menahan brute force dasar, namun tidak efektif untuk brute force terdistribusi atau skenario kredensial bocor.
Port Knocking	Yefta (2019); Setyowibowo dkk. (2022)	Port knocking hanya menyembunyikan port dan masih dapat ditembus jika urutan diketahui.
Intrusion Prevention System (IPS)	Usman dkk. (2024)	IPS bersifat reaktif dan bekerja pada lapisan jaringan, bukan autentikasi.

Tabel 2.2 memperlihatkan bahwa:

a. Tidak ada penelitian yang secara langsung mengimplementasikan MFA pada SSH Mikrotik, meskipun beberapa penelitian membuktikan bahwa MFA efektif untuk meningkatkan keamanan akses.
b. Sebagian penelitian berfokus pada proteksi jaringan (firewall, IDS/IPS, port knocking), bukan pada proteksi berbasis autentikasi.

c. Metode seperti port knocking atau IPS hanya bekerja sebagai mekanisme penghalang awal, tetapi tidak memberikan verifikasi ganda terhadap identitas pengguna, sehingga masih rentan jika kredensial berhasil ditebak.
d. Belum ada penelitian yang menggunakan OTP (One-Time Password) atau RADIUS secara khusus untuk memperkuat akses SSH pada Mikrotik.

Dengan demikian, penelitian ini mengisi celah penting dengan menguji dan menganalisis implementasi *Multi-Factor Authentication* (MFA) berbasis RADIUS + OTP pada SSH Mikrotik, yang belum pernah dikaji secara komprehensif dalam literatur yang ada.

2.3 Relevansi Penelitian

Serangan brute force merupakan salah satu metode penyerangan yang dilakukan dengan cara menebak kombinasi kredensial secara berulang hingga menemukan pasangan yang benar [2]. Teknik ini berbahaya karena tidak memerlukan kelemahan khusus pada sistem: selama penyerang memiliki akses ke layanan autentikasi, percobaan dapat terus dilakukan sampai berhasil. Jika mekanisme pembatasan percobaan login tidak diterapkan dengan baik, serangan brute force dapat membuka peluang bagi pihak tidak berwenang untuk mengambil alih sistem [3].

Dalam konteks administrasi jaringan, autentikasi jarak jauh umumnya dilakukan menggunakan protokol Secure Shell (SSH). SSH menyediakan kanal komunikasi yang terenkripsi sehingga data sensitif, termasuk kredensial, tidak dapat dibaca oleh pihak lain selama proses transmisi [8]. Protokol ini banyak digunakan oleh administrator untuk mengelola perangkat jaringan secara aman, karena selain mengamankan jalur komunikasi, SSH juga mendukung autentikasi berbasis kata sandi maupun kunci kriptografi.

Salah satu perangkat jaringan yang banyak memanfaatkan SSH untuk keperluan administrasi adalah MikroTik RouterOS, yaitu sistem operasi jaringan berbasis Linux yang menyediakan beragam fitur seperti routing, firewall, manajemen bandwidth, hotspot, dan VPN. Ketersediaan fitur yang lengkap serta biaya implementasi yang

relatif rendah membuat RouterOS sangat populer pada skala UMKM, kampus, hingga ISP. Namun demikian, tingginya penggunaan RouterOS juga membuatnya menjadi target umum bagi serangan brute force, terutama pada layanan SSH.

Untuk memperkuat proses autentikasi, salah satu pendekatan yang banyak digunakan adalah Multi-Factor Authentication (MFA), yaitu mekanisme verifikasi yang memerlukan lebih dari satu faktor pembuktian identitas. Kajian internasional mengenai penggunaan MFA pada perangkat jaringan menunjukkan perkembangan yang cukup pesat. Misalnya, sistem operasi Cisco IOS XR telah menyediakan dukungan MFA yang dapat diintegrasikan langsung pada proses autentikasi SSH, di mana kata sandi dikombinasikan dengan token kriptografis sebagai faktor tambahan [16]. Pendekatan ini terbukti mampu menurunkan efektivitas serangan brute force secara signifikan karena keberhasilannya tidak lagi bergantung hanya pada pasangan username dan password, melainkan memerlukan verifikasi kedua yang tidak mudah diretas [15]. Melalui MFA, pengguna perlu memberikan bukti tambahan, misalnya kode verifikasi unik (Timed One-Time Password atau TOTP) yang hanya berlaku dalam jangka waktu singkat. Dengan demikian, meskipun penyerang mengetahui kata sandi, mereka tetap tidak dapat mengakses sistem tanpa kode TOTP tersebut.

Dalam implementasi teknis pada jaringan, MFA umumnya dikombinasikan dengan protokol autentikasi terpusat seperti RADIUS. RADIUS memungkinkan proses Authentication, Authorization, and Accounting (AAA) dilakukan dari satu server sentral, sehingga pengelolaan identitas pengguna menjadi lebih terstruktur dan aman. Pada penelitian ini, mekanisme OTP diimplementasikan melalui layanan autentikasi RADIUS User Manager pada perangkat MikroTik. Kode TOTP dihasilkan menggunakan standar OATH-TOTP, yang memanfaatkan shared secret dan parameter waktu untuk membentuk kode numerik yang hanya dapat digunakan sekali. M’Raihi dkk. menjelaskan bahwa algoritma TOTP bekerja dengan menggabungkan shared secret dan timestamp sistem, sehingga setiap kode memiliki masa berlaku yang sangat singkat, biasanya sekitar 30 detik [9]. Pada sisi verifikasi, server RADIUS menghitung ulang OTP menggunakan kunci dan waktu yang sama, lalu mencocokkannya dengan

kode yang dimasukkan oleh pengguna. Dengan demikian, keberhasilan autentikasi sangat bergantung pada kesesuaian waktu dan shared secret, sehingga hanya pengguna yang memiliki aplikasi autentikator yang sah yang mampu menghasilkan kode OTP yang valid.

Pemilihan SSH sebagai objek utama penelitian didorong oleh tiga pertimbangan penting. Pertama, SSH merupakan protokol standar yang digunakan untuk melakukan administrasi jarak jauh pada router MikroTik secara aman, sehingga wajar apabila layanan ini menjadi sasaran serangan. Fauzi dkk. menunjukkan bahwa layanan FTP dan SSH pada MikroTik memiliki kerentanan terhadap brute force yang dapat membuka akses tidak sah dan berpotensi menyebabkan kebocoran data [14]. Kedua, pada mode interaktif, SSH mengirimkan setiap karakter yang diketik pengguna dalam paket IP tersendiri secara langsung. Pola pengiriman ini memungkinkan penyerang menganalisis jeda antar ketikan (*inter-keystroke timing*) berdasarkan waktu kedatangan paket. Dengan memanfaatkan informasi tersebut dan teknik statistik sederhana, panjang kata sandi maupun pola pengetikan pengguna dapat diperkirakan dari sesi SSH [17]. Selain itu, jika host key SSH tidak diverifikasi dengan benar, koneksi dapat dimanipulasi melalui serangan *man-in-the-middle* (MITM) untuk mencuri kredensial pengguna [18]. Ketiga, Bäumer dkk. menyoroti *Terrapin Attack*, yaitu teknik yang mengeksploitasi manipulasi nomor urut paket dalam protokol SSH. Mereka menemukan bahwa SSH tidak melakukan pengaturan ulang terhadap counter urutan pesan ketika enkripsi mulai digunakan, sehingga penyerang dapat menyisipkan atau menghapus paket pada awal sesi SSH tanpa terdeteksi. Kondisi ini memungkinkan pelanggaran integritas saluran SSH, seperti menonaktifkan fitur keamanan tertentu atau menurunkan algoritma kriptografi secara diam-diam [19].

Secara keseluruhan, konsep-konsep dasar tersebut menunjukkan bahwa serangan brute force dapat dicegah bukan hanya melalui proteksi jaringan, tetapi juga dengan memperkuat proses autentikasi pengguna. Oleh karena itu, penerapan MFA pada layanan SSH di lingkungan RouterOS menjadi langkah relevan yang dapat meningkatkan keamanan sistem secara menyeluruh.