202110370311345
Eureka Diaandisy
Prodi Informatika

ANALISIS DAN IMPLEMENTASI *MULTI-FACTOR AUTHENTICATION* (MFA) UNTUK MENCEGAH SERANGAN *BRUTE FORCE* PADA SSH MIKROTIK

Laporan Tugas Akhir

Diajukan Untuk Memenuhi Persyaratan Guna Meraih Gelar Sarjana
Strata 1 Informatika Universitas Muhammadiyah Malang

Eureka Diaandisy
202110370311345

Bidang Minat
(Sistem Keamanan Jaringan)

PROGRAM STUDI INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS MUHAMMADIYAH MALANG
2026

202110370311345
Eureka Diaandisy
Prodi Informatika

LEMBAR PERSETUJUAN

Analisis dan Implementasi Multi-Factor (MFA) Authentication untuk Mencegah Serangan Brute Force pada SSH MikroTik

TUGAS AKHIR

Sebagai Persyaratan Guna Meraih Gelar Sarjana Strata 1
Informatika Universitas Muhammadiyah Malang

Menyetujui,

Malang, *17 April 2026*

Dosen Pembimbing 1

Diah Risqiwati ST., MT.

NIP. 10814100545PNS.

202110370311345
Eureka Diaandisy
Prodi Informatika

LEMBAR PENGESAHAN

Analisis dan Implementasi Multi-Factor Authentication (MFA) untuk Mencegah Serangan Brute Force pada SSH MikroTik

TUGAS AKHIR

Sebagai Persyaratan Guna Meraih Gelar Sarjana Strata 1

InformatikaUniversitas Muhammadiyah Malang

Disusun Oleh :

EUREKA DIAANDISY

202110370311345

Tugas Akhir ini telah diuji dan dinyatakan lulus melalui sidang majelis penguji pada tanggal 17 April 2026

Menyetujui,

Dosen Pembimbing 1

Diah Risqiwati ST., MT.
NIP. 10814100545PNS.

Dosen Penguji 1

Ir. Agus Eko Minarno S.Kom., M.Kom. IPM.
NIP. 10814100540PNS.

Dosen Penguji 2

Lailatul Husniah S.ST., MT.
NIP. 10816120580PNS.

202110370311345
Eureka Diaandisy
Prodi Informatika

Mengetahui,
Ketua Jurusan Informatika

Ir. Agus Eko Minarno S.Kom., M.Kom. IPM.
NIP. 10814100540PNS.

202110370311345
Eureka Diaandisy
Prodi Informatika

LEMBAR PERNYATAAN

Yang bertanda tangan dibawah ini :

NAMA : EUREKA DIAANDISY

NIM : 202110370311345

FAK./JUR. : Informatika

Dengan ini saya menyatakan bahwa Tugas Akhir dengan judul **"Analisis dan Implementasi Multi-Factor Authentication (MFA) untuk Mencegah Serangan Brute Force pada SSH MikroTik"** beserta seluruh isinya adalah karya saya sendiri dan bukan merupakan karya tulis orang lain, baik sebagian maupun seluruhnya, kecuali dalam bentuk kutipan yang telah disebutkan sumbernya.

Demikian surat pernyataan ini saya buat dengan sebenar-benarnya. Apabila kemudian ditemukan adanya pelanggaran terhadap etika keilmuan dalam karya saya ini, atau ada klaim dari pihak lain terhadap keaslian karya saya ini maka saya siap menanggung segala bentuk resiko/sanksi yang berlaku.

Mengetahui,
Dosen Pembimbing

Diah Risqiwati ST., MT.

Malang, 17 April 2026
Yang Membuat Pernyataan

EUREKA DIAANDISY

202110370311345
Eureka Diaandisy
Prodi Informatika

Abstrak

Keamanan layanan SSH pada perangkat MikroTik memiliki peran penting dalam menjaga integritas jaringan, terutama terhadap ancaman serangan brute force yang dapat menyebabkan kompromi kredensial. Penelitian ini bertujuan menguji efektivitas penerapan Multi-Factor Authentication (MFA) berbasis One-Time Password (OTP) melalui RADIUS dan User Manager dalam meningkatkan keamanan akses SSH MikroTik. Metode penelitian menggunakan pendekatan Network Development Life Cycle (NDLC), yang meliputi tahap analisis, desain, dan simulasi prototipe dalam lingkungan virtualisasi menggunakan PNETLab. Pengujian dilakukan menggunakan simulasi serangan brute force dengan THC-Hydra pada dua kondisi, yaitu tanpa MFA dan dengan MFA. Hasil pengujian menunjukkan bahwa pada skenario tanpa MFA, penyerang berhasil memperoleh kredensial SSH dalam waktu sekitar 335 detik, sedangkan pada skenario dengan MFA, serangan tidak berhasil menembus autentikasi dan hanya menghasilkan kegagalan login berulang selama 332 detik. Evaluasi kinerja perangkat memperlihatkan bahwa penggunaan CPU dan bandwidth relatif stabil pada kedua skenario, dengan konsumsi CPU rata-rata 2% dan maksimum 14%, serta pemakaian bandwidth berada pada kisaran 9,41-9,59 Kb. Temuan ini membuktikan bahwa MFA mampu meningkatkan keamanan SSH MikroTik secara signifikan tanpa memberikan beban tambahan yang berarti terhadap sumber daya sistem. Penelitian ini menyarankan penerapan MFA sebagai lapisan keamanan tambahan pada lingkungan jaringan produksi serta membuka peluang pengembangan metode autentikasi lanjutan, seperti biometrik atau FIDO, untuk penelitian selanjutnya.

Kata Kunci: Multi-Factor Authentication, NDLC, SSH, MikroTik, Brute Force, RADIUS, OTP, Keamanan Jaringan.

202110370311345
Eureka Diaandisy
Prodi Informatika

Abstract

The security of SSH services on MikroTik devices plays a crucial role in maintaining network integrity, particularly against brute-force attacks that may compromise user credentials. This study aims to evaluate the effectiveness of implementing Multi-Factor Authentication (MFA) based on One-Time Passwords (OTP) through RADIUS and User Manager in enhancing SSH security on MikroTik. The research adopts the Network Development Life Cycle (NDLC) approach, consisting of the analysis, design, and prototype simulation stages within a virtualized environment using PNETLab. Testing was conducted by simulating brute-force attacks using THC-Hydra under two conditions: without MFA and with MFA. The results show that in the scenario without MFA, attackers successfully obtained SSH credentials in approximately 335 seconds, whereas in the MFA-enabled scenario, the attack failed to bypass authentication and resulted only in repeated login errors for 332 seconds. Performance evaluation also indicates that CPU and bandwidth usage remained relatively stable in both scenarios, with average CPU utilization at 2% and a maximum of 14%, while bandwidth usage ranged from 9.41 to 9.59 Kb. These findings demonstrate that MFA significantly enhances SSH security on MikroTik without imposing substantial overhead on system resources. The study recommends applying MFA as an additional security layer in production network environments and highlights opportunities for future development of advanced authentication methods such as biometrics or FIDO-based solutions.

Keywords: Multi-Factor Authentication, NDLC, SSH, MikroTik, Brute Force, RADIUS, OTP, Network Security.

202110370311345
Eureka Diaandisy
Prodi Informatika

LEMBAR PERSEMBAHAN

Puji syukur kehadirat Allah SWT atas segala limpahan rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan Tugas Akhir ini dengan baik. Penulis menyampaikan terima kasih yang sebesar-besarnya kepada seluruh pihak yang telah memberikan dukungan, baik secara langsung maupun tidak langsung, selama proses penyusunan Tugas Akhir ini:

1. Kepada Papa Mahur dan Mama Andis; Mas Ian dan Mbak Bella; Mas Mikal dan Mbak Imah; serta Mas Kaka, yang dengan ketulusan dan hati yang lapang telah meluangkan waktu, tenaga, dan kasih sayang untuk mendampingi penulis, baik secara fisik, spiritual, mental, maupun finansial.
2. Kepada Budhe Wandan, Mbak Ica, Mas Faris, dan Mas Irfan; serta Tante Cucut, Dek Apin, dan Dek Izhar yang dengan keikhlasan dan kehangatan hati telah memberikan tempat bernaung serta berbagai kebaikan berharga kepada penulis selama masa studi.
3. Kepada Ibu Dr. Diah Risqiwati, S.T., M.T., selaku dosen pembimbing, yang telah dengan tulus meluangkan waktu, memberikan bimbingan, serta menyampaikan berbagai masukan berharga kepada penulis dalam proses penyelesaian tugas akhir ini.
4. Kepada seluruh dosen pengajar Universitas Muhammadiyah Malang yang dengan sepenuh hati telah membagikan ilmu, bimbingan, dan dedikasi mereka kepada kami, khususnya kepada penulis sebagai mahasiswa.
5. Kepada sahabat KOSTPID yang selama ini menjadi sosok tempat, layaknya rumah yang menghadirkan kenyamanan, kebersamaan, dan kenangan yang tak terlupakan.

202110370311345
Eureka Diaandisy
Prodi Informatika

KATA PENGANTAR

Puji syukur kehadirat Allah SWT atas rahmat, taufik, dan hidayah-Nya sehingga penulis dapat menyelesaikan Tugas Akhir ini dengan baik. Tugas Akhir yang berjudul **"ANALISIS DAN IMPLEMENTASI MULTI-FACTOR AUTHENTICATION (MFA) UNTUK MENCEGA SERANGAN BRUTE FORCE PADA SSH MIKROTIK"**

Tugas Akhir ini disusun sebagai salah satu syarat untuk menyelesaikan studi pada Program Studi Informatika. Penelitian ini bertujuan untuk menganalisis efektivitas penerapan Multi-Factor Authentication (MFA) sebagai upaya peningkatan keamanan autentikasi pada layanan SSH MikroTik, khususnya dalam konteks mitigasi serangan brute force yang merupakan salah satu ancaman siber paling umum terhadap perangkat jaringan saat ini.

Penulis menyadari bahwa Tugas Akhir ini masih jauh dari sempurna. Oleh karena itu, kritik dan saran yang membangun sangat penulis harapkan demi perbaikan di masa mendatang. Semoga Tugas Akhir ini dapat memberikan manfaat bagi pembaca, khususnya dalam pengembangan ilmu pengetahuan di bidang keamanan jaringan.

Malang, 9 Desember 2025

Eureka Diaandisy

DAFTAR ISI

202110370311345
Eureka Diaandisy
Prodi Informatika

DAFTAR GAMBAR

202110370311345
Eureka Diaandisy
Prodi Informatika

DAFTAR TABEL

DAFTAR LAMPIRAN

DAFTAR PUSTAKA

[1] H. Haeruddin, S. E. Prasetyo, dan A. W. Kaharuddin, "Optimalisasi Keamanan Jaringan Di Era Digital menggunakan metode Zero Trust," *JOINT*, vol. 5, no. 3, hlm. 15–24, Des 2024, doi: 10.37253/joint.v5i3.9986.

[2] V. Grover, "An Efficient Brute Force Attack Handling Techniques for Server Virtualization," *SSRN Journal*, 2020, doi: 10.2139/ssrn.3564447.

[3] C. Pamungkas, P. Hendradi, D. Sasongko, dan A. Ghifari, "Analysis of Brute Force Attacks Using National Institute Of Standards And Technology (NIST) Methods on Routers," *INISTA*, vol. 5, no. 2, hlm. 115–125, Mei 2023, doi: 10.20895/inista.v5i2.1039.

[4] R. P. Aji, "Analisis Log Serangan Bruteforce Terhadap Web Server Nginx Pada Dasbor Sistem Pencatatan Log Teroptimasi Menggunakan Metode Investigasi Forensik," Des 2022, Diakses: 14 November 2025. [Daring]. Tersedia pada: https://dspace.uii.ac.id/handle/123456789/42416

[5] "2025-dbir-data-breach-investigations-report.pdf." Diakses: 14 November 2025. [Daring]. Tersedia pada: https://www.verizon.com/business/resources/Td8e/reports/2025-dbir-data-breach-investigations-report.pdf

[6] S. Sujalwo, "Manajemen Jaringan Komputer Dengan Menggunakan Mikrotik Router (Computer Network Management Used With Microtic Router)," *Komuniti: Jurnal Komunikasi dan Teknologi Informasi*, vol. 2, no. 2, hlm. 32–43.

[7] Y. Mulyanto dan A. Algi Fari, "ANALISIS KEAMANAN LOGIN ROUTER MIKROTIK DARI SERANGAN BRUTEFORCE MENGGUNAKAN METODE PENETRATION TESTING (Studi Kasus: SMK NEGERI 2 SUMBAWA)," *JINTEKS*, vol. 4, no. 3, hlm. 145–155, Agu 2022, doi: 10.51401/jinteks.v4i3.1897.

[8] D. J. Barrett dan R. E. Silverman, *SSH, the secure shell: the definitive guide*, 1st ed. Cambridge [Mass.]: O'Reilly, 2001.

[9] D. M'Raihi, J. Rydell, M. Pei, dan S. Machani, "TOTP: Time-Based One-Time Password Algorithm," Internet Engineering Task Force, Request for Comments RFC 6238, Mei 2011. doi: 10.17487/RFC6238.

[10] Y. Christian, "Analisis Sistem Pengamanan Akses Autentikasi Jaringan dengan Metode Port Knocking dan Action Tarpit pada Router Mikrotik," *telcomatics*, vol. 4, no. 1, hlm. 1–6, Jul 2019, doi: 10.37253/telcomatics.v4i1.586.

[11] B. Arifwidodo, Y. Syuhada, dan S. Ikhwan, "Analisis Kinerja Mikrotik Terhadap Serangan Brute Force Dan DDoS," *tc*, vol. 20, no. 3, hlm. 392–399, Agu 2021, doi: 10.33633/tc.v20i3.4615.

[12] A. P. Usman, R. Y. Bakti, dan M. A. Hayat, "Optimalisasi Sistem Keamanan SSH dari Serangan Brute Force Mengunakan Intrusion Prevention System pada Mikrotik," *ajst*, vol. 2, no. 1, hlm. 116–122, Apr 2024, doi: 10.57250/ajst.v2i1.380.

[13] S. Setyowibowo, S. Sujito, dan N. Moka, "Keamanan Jaringan Hotspot Dengan Simple Port Knocking Dan Automated Backup Menggunakan Mikrotik," *jikstik*, vol. 21, no. 4, Des 2022, doi: 10.32409/jikstik.21.4.3109.

[14] A. Fauzi, F. Firmansyah, dan T. A. A. Sandi, "Perancangan Keamanan Router Mikrotik Dari Serangan FTP Dan SSH Brute Force," *Infortech*, vol. 6, no. 1, hlm. 9–14, Jun 2024, doi: 10.31294/infortech.v6i1.21697.

[15] H. Haeruddin, S. E. Prasetyo, dan A. Mindy, "Implementasi Multi-Factor Authentication Untuk Optimalisasi Keamanan Akses Data Di PT.ABC," *JAMIKA*, vol. 15, no. 1, hlm. 85096, Feb 2025, doi: 10.34010/5rdjmw37.

[16] "System Security Configuration Guide for Cisco NCS 5500 Series Routers, IOS XR Release 24.1.x, 24.2.x, 24.3.x, 24.4.x - Implementing Secure Shell [Cisco Network Convergence System 5500 Series]," Cisco. Diakses: 14 November 2025. [Daring]. Tersedia pada: https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/security/24xx/configuration/guide/b-system-security-cg-ncs5500-24xx/implementing-secure-shell.html

[17] D. X. Song, D. Wagner, dan X. Tian, "Timing Analysis of Keystrokes and Timing Attacks on {SSH}," dipresentasikan pada 10th USENIX Security

Symposium (USENIX Security 01), 2001. Diakses: 13 November 2025. [Daring]. Tersedia pada: https://www.usenix.org/conference/10th-usenix-security-symposium/timing-analysis-keystrokes-and-timing-attacks-ssh

[18] R. Andrews, D. A. Hahn, dan A. G. Bardas, "Measuring the Prevalence of the Password Authentication Vulnerability in SSH," dalam *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, Dublin, Ireland: IEEE, Jun 2020, hlm. 1–7. doi: 10.1109/ICC40277.2020.9148912.

[19] F. Bäumer, M. Brinkmann, dan J. Schwenk, "Terrapin Attack: Breaking SSH Channel Integrity By Sequence Number Manipulation," 8 Mei 2024, *arXiv*: arXiv:2312.12422. doi: 10.48550/arXiv.2312.12422.

[20] F. Naim, Rd. R. Saedudin, dan U. Y. K. S. Hediyanto, "ANALYSIS OF WIRELESS AND CABLE NETWORK QUALITY-OF-SERVICE PERFORMANCE AT TELKOM UNIVERSITY LANDMARK TOWER USING NETWORK DEVELOPMENT LIFE CYCLE (NDLC) METHOD," *jipi. jurnal. ilmiah. penelitian. dan. pembelajaran. informatika.*, vol. 7, no. 4, hlm. 1033–1044, Nov 2022, doi: 10.29100/jipi.v7i4.3192.

[21] Y. Ardiansyah, U. Y. Kurnia Septo Hediyanto, dan M. T. Kurniawan, "ANALISIS DAN OPTIMASI TEKNOLOGI JARINGAN WIRELESS PADA RUANGAN PROSES MANUFAKTUR DI GEDUNG MANGUDU UNIVERSITAS TELKOM DENGAN MENGGUNAKAN WIRELESS SITE SURVEY," *jipi. jurnal. ilmiah. penelitian. dan. pembelajaran. informatika.*, vol. 9, no. 2, hlm. 529–539, Mei 2024, doi: 10.29100/jipi.v9i2.4483.

[22] S. Donaldson, N. Coull, dan D. McLuskie, "A methodology for testing virtualisation security," dalam *2017 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, London, United Kingdom: IEEE, Jun 2017, hlm. 1–8. doi: 10.1109/CyberSA.2017.8073397.

[23] C. A. Hamka, H. Sajati, dan Y. Indrianingsih, "SISTEM KEAMANAN JAIL BASH UNTUK MENGAMANKAN AKUN LEGAL DARI KEJAHATAN

INTERNET MENGGUNAKAN THC-HYDRA," *Compiler*, vol. 3, no. 1, Mei 2014, doi: 10.28989/compiler.v3i1.63.

[24] Yopi Hidayatul Akbar, "Evaluasi Keamanan Jaringan Wireless Hotspot Menggunakan Metode Square (Studi Kasus Warnet Medianet Sumedang)," *Infoman's*, vol. 9, no. 2, hlm. 75–90, 2015, doi: 10.33481/infomans.v9i2.60.

[25] M. Cezar, "How to Find All Failed SSH login Attempts in Linux." Diakses: 18 Juni 2025. [Daring]. Tersedia pada: https://www.tecmint.com/find-failed-ssh-login-attempts-in-linux/

[26] "Login failure on log - RouterOS / Beginner Basics," MikroTik community forum. Diakses: 18 Juni 2025. [Daring]. Tersedia pada: https://forum.mikrotik.com/t/login-failure-on-log/111336

[27] L. Meyer, S. Romero, G. Bertoli, T. Burt, A. Weinert, dan J. Lavista Ferres, *How effective is multifactor authentication at deterring cyberattacks?* 2023. doi: 10.48550/arXiv.2305.00945.

[28] "How to Stop Brute Force Attacks with WordPress OTP," Shield Security. Diakses: 18 Juni 2025. [Daring]. Tersedia pada: https://getshieldsecurity.com/blog/wordpress-one-time-password/

[29] R. George dan E. Z. Abay, *Detection of SSH Brute-Force Attacks Using Machine Learning : A Comparative Study with Fail2Ban and PAM Tally2*. 2025. Diakses: 13 November 2025. [Daring]. Tersedia pada: https://urn.kb.se/resolve?urn=urn:nbn:se:hv:diva-23725

[30] D. Patel, D. Trivedi, U. Raval, dan A. Dennisan, "2F-Authsys: A hyperlocal two-factor authentication system using Near Sound Data Transfer," *JART*, vol. 22, no. 2, hlm. 197–205, Apr 2024, doi: 10.22201/icat.24486736e.2024.22.2.2244.

[31] "Bruteforce prevention - RouterOS - MikroTik Documentation." Diakses: 18 Juni 2025. [Daring]. Tersedia pada: https://help.mikrotik.com/docs/spaces/ROS/pages/268337176/Bruteforce+prevention

[32] B. Kondracki, B. A. Azad, O. Starov, dan N. Nikiforakis, "Catching Transparent Phish: Analyzing and Detecting MITM Phishing Toolkits," dalam *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, dalam CCS '21. New York, NY, USA: Association for Computing Machinery, Nov 2021, hlm. 36–50. doi: 10.1145/3460120.3484765.

[33] R. Soni, "Understanding OTP Authentication: HOTP & TOTP Explained," LoginRadius. Diakses: 14 November 2025. [Daring]. Tersedia pada: https://www.loginradius.com/blog/identity/what-is-otp-authentication

[34] S. Rose, O. Borchert, S. Mitchell, dan S. Connelly, "Zero Trust Architecture," National Institute of Standards and Technology, Agu 2020. doi: 10.6028/NIST.SP.800-207.

UNIVERSITAS MUHAMMADIYAH MALANG

FAKULTAS TEKNIK

INFORMATIKA
informatika.umm.ac.id | informatika@umm.ac.id

FORM CEK PLAGIARISME LAPORAN TUGAS AKHIR

Nama Mahasiswa : Eureka Diaandisy

NIM : 202110370311345

Judul TA : Analisis dan Implementasi Multi-Factor Authentication (MFA) untuk Mencegah Serangan Brute Force pada SSH MikroTik

Hasil Cek Plagiarisme dengan Turnitin

No.	Komponen Pengecekan	Nilai Maksimal Plagiarisme (%)	Hasil Cek Plagiarisme (%) *
1.	Bab 1 – Pendahuluan	10 %	5 %
2.	Bab 2 – Daftar Pustaka	25 %	0 %
3.	Bab 3 – Analisis dan Perancangan	25 %	2 %
4.	Bab 4 – Implementasi dan Pengujian	15 %	0 %
5.	Bab 5 – Kesimpulan dan Saran	5 %	3 %
6.	Makalah Tugas Akhir	20%	14 %

) Hasil cek plagiarism diisi oleh pemeriksa (staf TU)

***) Maksimal 5 kali (4 Kali sebelum ujian, 1 kali sesudah ujian)**

Mengetahui,

Pemeriksa (Staff TU)

(.....FITRI.....)

Kampus I
Jl. Bandung 1 Malang, Jawa Timur
P. +62 341 551 253 (Hunting)
F. +62 341 460 435

Kampus II
Jl. Bendungan Sutami No 188 Malang, Jawa Timur
P. +62 341 551 149 (Hunting)
F. +62 341 582 060

Kampus III
Jl. Raya Tlogomas No 246 Malang, Jawa Timur
P. +62 341 464 318 (Hunting)
F. +62 341 460 435
E. webmaster@umm.ac.id