e-ISSN : 2722-4368

Strategi Keamanan Router MikroTik: Deteksi dan Mitigasi Serangan Brute Force Berbasis Scripting

Ardiansyah[1*], Andi Asvin Mahersatillah Suradi[2], Wahyuddin Saputra[3]
Politeknik Negeri Ujung Pandang, Jl. Perintis Kemerdekaan KM. 10, Makassar, Indonesia[123]
Email coresponden: ardi.zainal@poliupg.ac.id

Abstrak. *Serangan brute force merupakan salah satu ancaman keamanan utama terhadap perangkat jaringan, termasuk router MikroTik. Teknik ini memungkinkan penyerang mendapatkan akses tidak sah dengan mencoba berbagai kombinasi username dan password secara berulang. Meskipun MikroTik memiliki fitur keamanan bawaan, serangan brute force tetap menjadi tantangan bagi administrator jaringan, terutama pada layanan yang sering digunakan untuk akses remote seperti SSH, Telnet, FTP, Winbox, WWW, dan API. Penelitian ini bertujuan untuk mengembangkan metode deteksi dan mitigasi serangan brute force secara lebih dinamis dengan memanfaatkan scripting MikroTik. Metode yang diusulkan mengidentifikasi pola serangan berdasarkan jumlah percobaan login yang dilakukan serta karakteristik pengguna. Hasil penelitian menunjukkan bahwa metode ini berhasil mendeteksi dan mitigasi serangan brute force secara signifikan pada berbagai layanan login router dalam periode 28 Januari - 4 Februari 2025, sehingga meningkatkan keamanan jaringan secara keseluruhan. Dengan demikian, pendekatan ini diharapkan dapat menjadi solusi efektif bagi administrator jaringan dalam menghadapi ancaman serangan brute force yang semakin kompleks.*

Kata Kunci : Keamanan Jaringan, MikroTik, Brute Force, Scripting.

Abstract. *Brute force attacks represent one of the primary security threats to network devices, including MikroTik routers. This technique allows attackers to gain unauthorized access by repeatedly trying various combinations of usernames and passwords. Although MikroTik has built-in security features, brute force attacks remain a challenge for network administrators, particularly on services frequently used for remote access such as SSH, Telnet, FTP, Winbox, WWW, and API. This research aims to develop a more dynamic method for detecting and mitigating brute force attacks by leveraging MikroTik scripting. The proposed method identifies attack patterns based on the number of login attempts made and user characteristics. The research results show that this method successfully detected and mitigated brute force attacks significantly on various router login services during the period of January 28 - February 4, 2025, thereby enhancing overall network security. Thus, this approach is expected to serve as an effective solution for network administrators in addressing increasingly complex brute force attack threats.*

Keywords : Network Security, MikroTik, Brute Force, Scripting.

PENDAHULUAN

Router MikroTik merupakan salah satu perangkat jaringan yang sering menjadi target serangan *brute force* saat ini. Serangan *brute force* adalah teknik yang digunakan oleh penyerang untuk mendapatkan akses tidak sah dengan mencoba berbagai kombinasi *username* dan *password* secara berulang. Metode ini dapat menyebabkan kerugian signifikan, termasuk pencurian data dan kerusakan sistem, sehingga menjadi perhatian utama bagi *Administrator* jaringan [1][2]. Penelitian menunjukkan bahwa serangan ini semakin canggih dan sering kali berhasil menembus sistem keamanan yang ada, sehingga diperlukan pendekatan baru untuk mendeteksinya secara efektif [3]

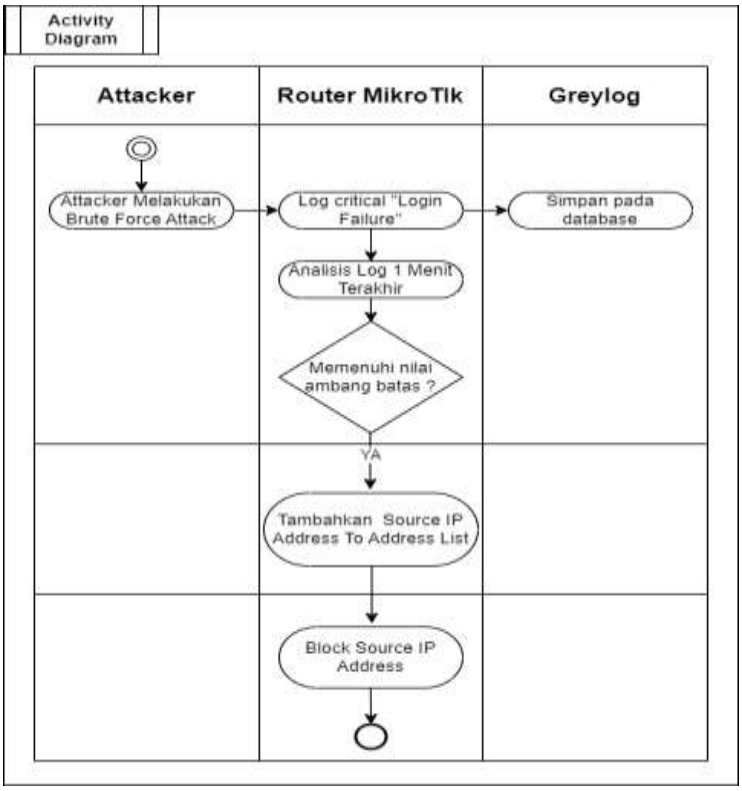
Router MikroTik dipilih sebagai fokus penelitian ini karena popularitas dan keandalannya dalam berbagai aplikasi jaringan, baik di lingkungan rumah tangga maupun perusahaan. *Router*

MikroTik menawarkan berbagai fitur yang memungkinkan administrator untuk mengelola dan mengamankan jaringan dengan lebih baik. Namun, meskipun memiliki banyak keunggulan, router MikroTik juga rentan terhadap serangan *brute force*, terutama pada layanan seperti *SSH*, *Telnet*, *API* dan *FTP* yang secara *default* terbuka, yang sering digunakan untuk mengakses perangkat secara remote [4] [5]. Penelitian sebelumnya menunjukkan bahwa banyak serangan *brute force* yang berhasil dilakukan melalui protokol ini, sehingga penting untuk mengembangkan solusi yang lebih efektif untuk melindungi perangkat [6] [7].

Dalam konteks ini, terdapat beberapa penelitian yang telah dilakukan terkait dengan serangan *brute force* pada *router*, Menekankan bahwa pengamanan router dengan *firewall* dan penerapan metode forensik digital, seperti pendekatan NIST [8], sangat penting dalam mendeteksi serta mencegah serangan *brute force*, yang dapat mengancam keamanan jaringan dan aktivitas akademik di institusi pendidikan. termasuk analisis keamanan dan pengujian penetrasi untuk mengidentifikasi kerentanan pada layanan *SSH* dan *Telnet* [5] [9]. Namun, sebagian besar penelitian ini masih menggunakan metode yang statis dan tidak mempertimbangkan variabel dinamis dalam pendeteksian serangan. Oleh karena itu, pada penelitian ini akan pengembangan metode yang lebih dinamis dengan memanfaatkan *scripting MikroTik* untuk mendeteksi serangan *brute force* berdasarkan jumlah percobaan login yang dilakukan dan karakteristik pengguna [10].

Tujuan dari penelitian ini adalah untuk merancang metode baru dalam pendeteksian serangan brute force pada *router MikroTik* yang lebih dinamis. Metode ini akan menggunakan variabel unik untuk setiap pengguna dan jumlah percobaan *login* yang dilakukan untuk mengidentifikasi pola serangan secara lebih efektif. Dengan pendekatan ini, diharapkan dapat meningkatkan respons terhadap serangan *brute force* dan memperkuat keamanan jaringan secara keseluruhan [7][11]. Penelitian ini diharapkan dapat memberikan kontribusi signifikan terhadap pengembangan strategi keamanan yang lebih baik untuk *router MikroTik* dan perangkat jaringan lainnya.

METODOLOGI PENELITIAN



Gambar 1. *ACTIVITY diagram* Proses sistem

e-ISSN : 2722-4368

Gambar 1 di atas menunjukkan bawah alur Metode penelitian yang digunakan dalam studi ini berfokus pada pengembangan pendekatan dinamis untuk mendeteksi dan mendeteksi serangan *brute force* pada perangkat *router MikroTik*. Penelitian ini memanfaatkan *scripting MikroTik* untuk mengidentifikasi pola serangan berdasarkan jumlah percobaan login gagal serta karakteristik pengguna, seperti frekuensi akses dan sumber IP. Script yang dikembangkan secara otomatis memantau aktivitas login pada layanan jaringan (*SSH, Telnet, FTP, WinBox, WWW, API*) dan menerapkan mitigasi dengan memblokir atau membatasi akses dari sumber yang mencurigakan setelah melewati ambang batas tertentu.

Fungsi logika yang digunakan untuk mendeteksi serangan *brute force* dirumuskan sebagai berikut:

$$F(x,y) = \begin{cases} 1, & jika\ x \geq 10 \wedge y \geq 3 \\ 0, & lainnya \end{cases}$$

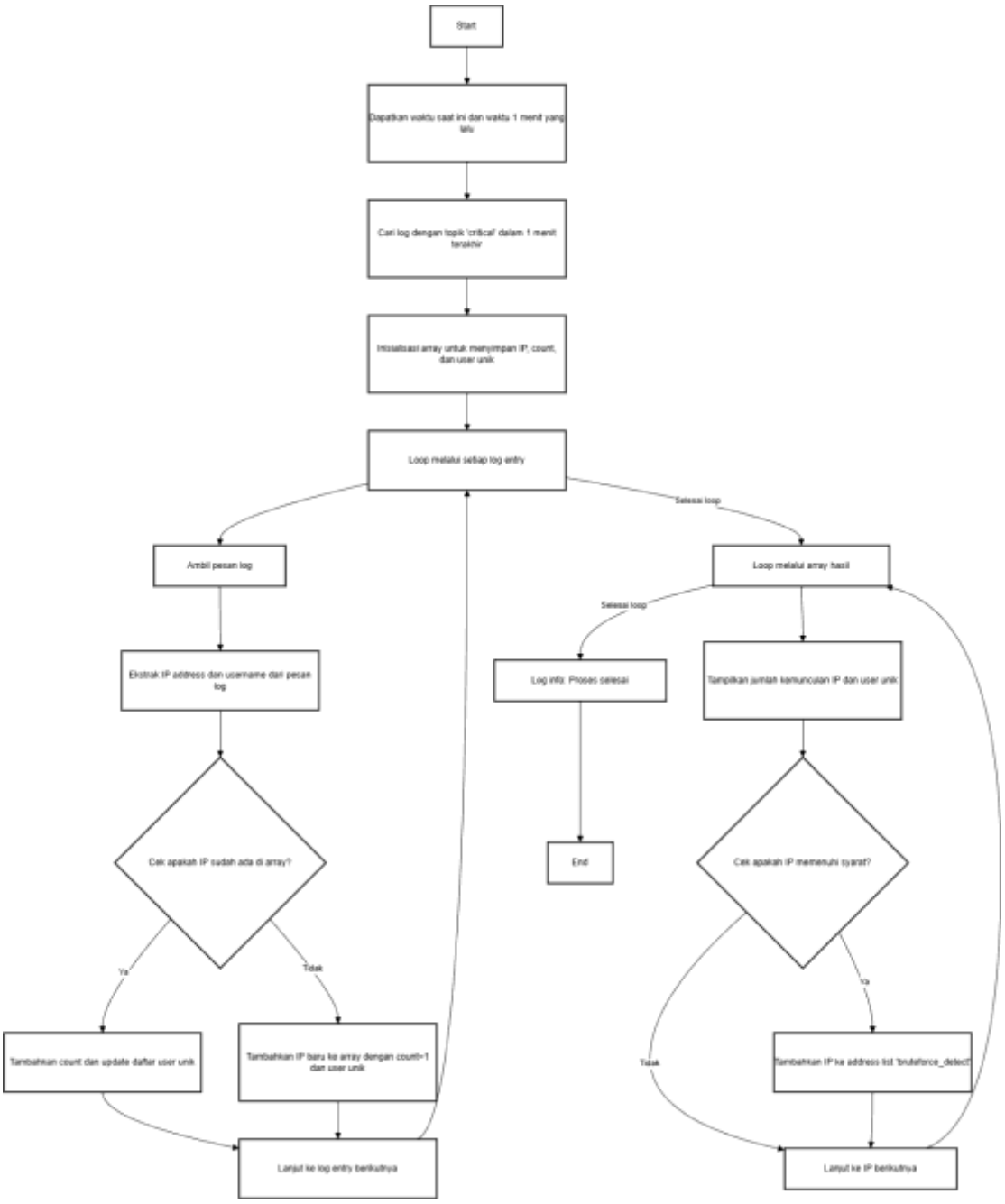
Keterangan:

- x adalah jumlah kesalahan login
- y adalah jumlah user yang berbeda yang digunakan untuk kesalahan login
- F(x, y) adalah fungsi yang mengembalikan nilai 1 jika terdapat serangan brute force dan 0 jika tidak.

Dasar pemilihan ambang batas x ≥ 10 dan y ≥ 3 didasarkan pada hasil eksperimen yang dilakukan dalam rentang waktu 1 menit. Dari pengujian yang dilakukan, pola ini menunjukkan bahwa serangan *brute force* cenderung mencoba berbagai kombinasi *username* dalam waktu singkat dengan tingkat kegagalan login yang tinggi. Dengan demikian, parameter ini diidentifikasi sebagai indikator utama dalam mendeteksi serangan *brute force* pada *router MikroTik*.

Kode ditulis dalam bahasa scripting MikroTik RouterOS dan bertujuan untuk mengidentifikasi aktivitas login mencurigakan dengan memantau *log* sistem dan menambahkan sumber *IP address* yang terdeteksi ke dalam daftar *address lists* jika memenuhi kriteria tertentu. Berikut penjelasan tahapan flowchart pada Gambar 2:

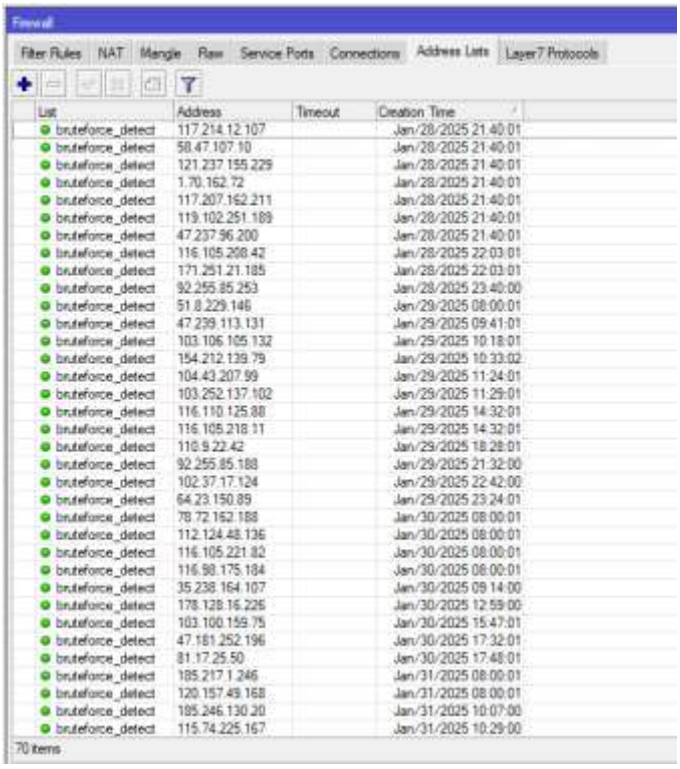
1. Mengambil log dengan topik “critica”’ dalam 1 menit terakhir
2. Mendapatkan waktu saat ini dan rentang waktu 1 menit sebelumnya
3. Mencari log dengan topik critical dalam rentang waktu 1 menit terakhir
4. Inisialisasi array untuk penyimpanan data
5. Memproses setiap log yang ditemukan
6. Ekstraksi ip address dan username dari pesan log
7. Memperbarui atau menambahkan data ke array
8. Menampilkan hasil analisis
9. Menambahkan ip ke daftar address lists jika memenuhi kriteria brute force attack (≥ 10 kemunculan dan ≥ 3 user unik)



Gambar 2. *Flowchart* Pendeteksian Serangan *Bruteforce*

HASIL DAN PEMBAHASAN

Hasil pengujian menunjukkan bahwa pendekatan yang diusulkan mampu secara efektif mengidentifikasi pola serangan berdasarkan jumlah percobaan login gagal, serta karakteristik pengguna seperti frekuensi akses dan alamat IP sumber. Pengujian dilakukan pada periode 28 Januari - 4 Februari 2025, dengan data log kegagalan login dikumpulkan menggunakan Graylog guna untuk membantu dalam proses visualisasi pola serangan *brute force*. Pada Gambar 3. Merupakan hasil deteksi serangan *brute force* dengan menggunakan *MikroTik Scripting* yang telah pasangkan pada *router MikroTik, source IP Address* penyerang secara otomatis akan ditambahkan ke *Address Lists* pada router, yang nantinya akan digunakan *firewall filter* untuk dilakukan *blocking*.



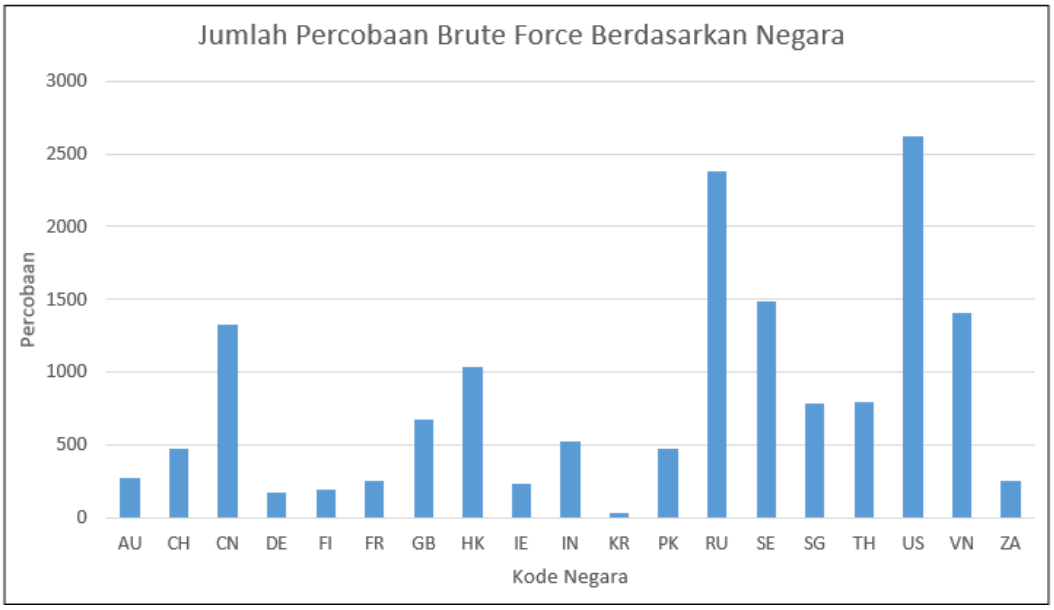
Gambar 3. Daftar *Source IP Address brute force* pada *address lists MikroTik*

Berikut hasil analisis data serangan *brute force* yang masuk pada *router mikroTik*:

Tabel 1. Daftar IP Address Penyerang dan Asal Negara

No	IP Address	Kode Negara	Jumlah Percobaan	No	IP Address	Kode Negara	Jumlah Percobaan
1	117.214.12.107	IN	12	**36**	164.92.85.77	US	318
2	58.47.107.10	CN	54	**37**	194.164.124.225	GB	312
3	121.237.155.229	CN	90	**38**	143.198.81.64	SG	215
4	1.70.162.72	CN	19	**39**	103.25.139.186	PK	469
5	117.207.162.211	IN	39	**40**	146.190.220.159	US	74
6	119.102.251.189	CN	13	**41**	220.194.171.236	CN	67
7	47.237.96.200	SG	40	**42**	77.105.177.106	RU	206
8	116.105.208.42	VN	81	**43**	103.77.215.124	VN	75
9	171.251.21.185	VN	62	**44**	211.149.173.141	CN	928
10	92.255.85.253	RU	1936	**45**	143.110.157.62	US	290
11	51.8.229.146	US	221	**46**	116.105.218.150	VN	81
12	47.239.113.131	HK	325	**47**	171.251.20.61	VN	81
13	103.106.105.132	VN	248	**48**	51.158.71.166	FR	250
14	154.212.139.79	TH	412	**49**	106.75.165.53	CN	23
15	104.43.207.99	US	100	**50**	174.138.36.168	US	250
16	103.252.137.102	VN	27	**51**	116.110.64.108	VN	69
17	116.110.125.88	VN	78	**52**	116.110.21.185	VN	73
18	116.105.218.11	VN	76	**53**	34.94.79.79	US	230
19	110.9.22.42	KR	36	**54**	103.104.211.104	IN	468

No	IP Address	Kode Negara	Jumlah Percobaan	No	IP Address	Kode Negara	Jumlah Percobaan
20	92.255.85.188	RU	115	**55**	77.91.103.192	FI	13
21	102.37.17.124	ZA	250	**56**	47.76.140.191	HK	250
22	64.23.150.89	US	248	**57**	146.235.234.85	US	137
23	78.72.162.188	SE	71	**58**	125.26.161.58	TH	387
24	112.124.48.136	CN	135	**59**	52.169.25.196	IE	233
25	116.105.221.82	VN	80	**60**	134.209.22.126	GB	274
26	116.98.175.184	VN	68	**61**	116.110.10.31	VN	77
27	35.238.164.107	US	196	**62**	116.110.113.56	VN	74
28	178.128.16.226	SG	248	**63**	62.164.223.39	DE	175
29	103.100.159.75	HK	459	**64**	65.108.222.134	FI	177
30	47.181.252.196	US	413	**65**	134.209.120.69	US	148
31	81.17.25.50	CH	473	**66**	116.110.19.93	VN	132
32	185.217.1.246	SE	943	**67**	112.213.39.74	AU	248
33	120.157.49.168	AU	21	**68**	139.59.127.12	SG	281
34	185.246.130.20	SE	472	**69**	92.255.85.189	RU	119
35	115.74.225.167	VN	20	**70**	194.0.234.37	GB	88



Gambar 4. Jumlah percobaan berdasarkan asal negara

Tabel 2. 50 User yang paling sering digunakan

No	User	Jumlah	No	User	Jumlah
1	root	9676	**26**	dev	128
2	admin	2420	**27**	tomcat	128
3	user	1189	**28**	steam	125
4	oracle	492	**29**	user1	123
5	ubuntu	476	**30**	lighthouse	123
6	test	422	**31**	elastic	121
7	www	291	**32**	oscar	118
8	debian	281	**33**	uftp	118

No	User	Jumlah	No	User	Jumlah
9	user2	232	**34**	dolphinscheduler	117
10	ftpuser	230	**35**	deploy	116
11	ftp	227	**36**	sonar	114
12	guest	209	**37**	tom	109
13	gitlab	203	**38**	pi	107
14	postgres	200	**39**	anonymous	104
15	es	194	**40**	apache	99
16	ubnt	177	**41**	support	97
17	hadoop	175	**42**	data	96
18	flask	173	**43**	Admin	92
19	git	163	**44**	developer	88
20	mysql	149	**45**	gpadmin	87
21	default	146	**46**	flink	84
22	esuser	140	**47**	administrator	82
23	app	140	**48**	observer	81
24	wang	136	**49**	centos	81
25	nginx	132	**50**	zabbix	80

Gambar 5. *Heatmap* Jumlah serangan *Brute Force* Berdasarkan Jam dalam Sehari.

KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan, dapat disimpulkan bahwa metode deteksi dan mitigasi serangan *brute force* menggunakan *scripting MikroTik* terbukti efektif dalam meningkatkan keamanan jaringan. Pendekatan ini berhasil mengidentifikasi pola serangan dengan memanfaatkan variabel dinamis, seperti jumlah percobaan login gagal dan karakteristik pengguna, yang diimplementasikan melalui fungsi logika. Pengujian yang dilakukan pada periode 28 Januari – 4 Februari 2025 menunjukkan bahwa metode ini mampu mendeteksi aktivitas mencurigakan dari berbagai *Source IP Address*, dengan beberapa IP mencatat jumlah percobaan login gagal yang sangat tinggi, seperti 1936 percobaan dari IP 92.255.85.253. Selain itu, analisis terhadap nama pengguna yang paling sering digunakan dalam serangan *brute force* menunjukkan bahwa nama pengguna umum seperti *root, admin*, dan *user* menjadi target utama penyerang.

Meskipun metode deteksi dan mitigasi serangan *brute force* menggunakan *scripting MikroTik* terbukti efektif dalam meningkatkan keamanan jaringan, penelitian ini memiliki beberapa keterbatasan yaitu di mana *script* akan dijalankan setiap 1 menit, yang berarti proses deteksi dan penambahan *address lists* dilakukan secara berkala, bukan secara real-time. Hal ini dapat menyebabkan jeda dalam respons terhadap serangan yang sangat cepat. Semakin banyak *source IP Address* yang terdeteksi dan dimasukkan ke dalam *address list*, semakin besar konsumsi sumber daya pada *router*, yang berpotensi memengaruhi performa sistem, terutama pada perangkat dengan spesifikasi terbatas. Untuk mengurangi dampak penggunaan sumber daya, di masa depan dapat

diterapkan mekanisme deteksi berbasis event-driven atau menggunakan *threshold* dinamis untuk mengoptimalkan efisiensi sistem.

DAFTAR PUSTAKA

[1] A. Henry *et al.*, "Composition of Hybrid Deep Learning Model and Feature Optimization for Intrusion Detection System," *Sensors*, vol. 23, no. 2, p. 890, 2023, doi: 10.3390/s23020890.

[2] R. J. Putra, N. P. Sastra, and D. M. Wiharta, "Pengembangan Komunikasi Multikanal Untuk Monitoring Infrastruktur Jaringan Berbasis Bot Telegram," *Jurnal Spektrum*, vol. 5, no. 2, p. 152, 2018, doi: 10.24843/spektrum.2018.v05.i02.p19.

[3] H. Husain, "Implementation of Port Knocking With Telegram Notifications to Protect Against Scanner Vulnerabilities," *Matrik Jurnal Manajemen Teknik Informatika Dan Rekayasa Komputer*, vol. 23, no. 1, pp. 215–228, 2023, doi: 10.30812/matrik.v23i1.3459.

[4] G. Suseela, Y. A. V Phamila, G. Niranjana, K. Ramana, S. Singh, and B. Yoon, "Low Energy Interleaved Chaotic Secure Image Coding Scheme for Visual Sensor Networks Using Pascal's Triangle Transform," *Ieee Access*, vol. 9, pp. 134576–134592, 2021, doi: 10.1109/access.2021.3116111.

[5] H. Haeruddin, "Analisa Dan Implementasi Sistem Keamanan Router Mikrotik Dari Serangan Winbox Exploitation, Brute-Force, DoS," *Jurnal Media Informatika Budidarma*, vol. 5, no. 3, p. 848, 2021, doi: 10.30865/mib.v5i3.2979.

[6] B. I. Farhan and A. D. Jasim, "Improving Detection for Intrusion Using Deep LSTM With Hybrid Feature Selection Method," *Iraqi Journal of Information & Communications Technology*, vol. 6, no. 1, pp. 40–50, 2024, doi: 10.31987/ijict.6.1.213.

[7] K. Hynek, T. Beneš, T. Čejka, and H. Kubátová, "Refined Detection of SSH Brute-Force Attackers Using Machine Learning," pp. 49–63, 2020, doi: 10.1007/978-3-030-58201-2_4.

[8] C. Pamungkas, P. Hendradi, D. Sasongko, and A. Ghifari, "Analysis of Brute Force Attacks Using National Institute Of Standards And Technology (NIST) Methods on Routers," *Journal of Informatics Information System Software Engineering and Applications (INISTA)*, vol. 5, no. 2, pp. 115–125, May 2023, doi: 10.20895/inista.v5i2.1039.

[9] M. Catillo, A. Pecchia, and U. Villano, "Measurement-Based Analysis of a DoS Defense Module for an Open Source Web Server," pp. 121–134, 2020, doi: 10.1007/978-3-030-64881-7_8.

[10] H. Liu and P. Patras, "NetSentry: A Deep Learning Approach to Detecting Incipient Large-Scale Network Attacks," 2022, doi: 10.48550/arxiv.2202.09873.

[11] S. F. Ghazal and S. A. Mjlae, "Cybersecurity in Deep Learning Techniques: Detecting Network Attacks," *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 11, 2022, doi: 10.14569/ijacsa.2022.0131125.