JIMU: Jurnal Ilmiah Multi Disiplin
Vol. 03, N0. 01, Tahun 2025, Hal. 76 - 85, ISSN: 3031-9498 (Online)

Implementasi Log Mikrotik Berbasis Database PostgreSQL dengan Teknologi Logging Syslog terhadap Serangan Brute Force

Nur Fadilla Inggriani. T[1], Jumadi M. Parenreng[2], Muh. Syahid Nur Wahid[3]
[1,2,3] Universitas Negeri Makassar
Email: fadillainggriani@gmail.com

Article Info

Article history:

Received September 25, 2024
Revised October 06, 2024
Accepted October 08, 2024

Keywords:

bot telegram, DDoS, firewall raw, MikroTik router, monitoring.

ABSTRACT

Network security is an important aspect in the digital era, especially in facing the threat of brute force attacks which often target network devices such as Mikrotik. Brute force attacks attempt to gain unauthorized access by trying various username and password combinations. This research aims to develop a system for monitoring and recording brute force attacks on Mikrotik devices, utilizing Syslog technology and integration with the PostgreSQL database. This system uses a firewall as an initial defense to block attacks before they reach the internal network. Blocked attack logs are then logged and stored in a PostgreSQL database for further analysis purposes. The research results show that this system is able to detect brute force attacks effectively and provide structured log information, thereby significantly improving network security.

Article Info

Article history:

Received September 25, 2024
Revised October 06, 2024
Accepted October 08, 2024

Keywords:

bot telegram, DDoS, firewall raw, MikroTik router, monitoring.

ABSTRACT

Keamanan jaringan menjadi aspek penting di era digital, terutama dalam menghadapi ancaman serangan brute force yang sering menargetkan perangkat jaringan seperti Mikrotik. Serangan brute force berupaya mendapatkan akses tidak sah dengan mencoba berbagai kombinasi username dan password. Penelitian ini bertujuan untuk mengembangkan sistem monitoring dan pencatatan serangan brute force pada perangkat Mikrotik, memanfaatkan teknologi Syslog dan integrasi dengan database PostgreSQL. Sistem ini menggunakan firewall sebagai pertahanan awal untuk memblokir serangan sebelum mencapai jaringan internal. Log serangan yang diblokir kemudian dicatat dan disimpan dalam database PostgreSQL untuk keperluan analisis lebih lanjut. Hasil penelitian menunjukkan bahwa sistem ini mampu mendeteksi serangan brute force secara efektif dan memberikan informasi log yang terstruktur, sehingga dapat meningkatkan keamanan jaringan secara signifikan.

Corresponding Author:

Nama penulis: Nur Fadilla Inggriani. T
Universitas Negeri Makassar
Email: fadillainggriani@gmail.com

Pendahuluan

Kemajuan internet di era ini, keamanan jaringan menjadi aspek krusial untuk memastikan integritas dan keberlanjutan data. Namun, di tengah perkembangan teknologi *router* yang pesat, perangkat *router*, khususnya *router* Mikrotik, menjadi sangat vital bagi penyedia layanan internet dalam pembangunan dan pengamanan jaringan mereka. Router sering menjadi target utama bagi pihak yang bermaksud jahat untuk merusak kinerjanya (Sayuti & Gunawan, 2023).

Keamanan jaringan adalah suatu sistem yang menghalangi aktivitas yang tidak diinginkan dengan mengenali pengguna yang tidak memiliki hak akses ke jaringan. Menghubungkan komputer Anda dengan komputer lain melalui jaringan kabel atau nirkabel dapat memungkinkan orang lain untuk mengakses data, mengubah konten, bahkan menghapus data secara daring. Potensi kerentanan dapat ditemui di berbagai elemen, mulai dari perangkat dan jalur data hingga aplikasi dan pengguna. (Istiqamah & Parenreng, 2023).

Ancaman serangan siber, terutama serangan *Brute force*, menjadi salah satu ancaman serius terhadap keamanan *server* dan router. Serangan *Brute force* merupakan suatu metode yang dilakukan oleh penyerang dengan mencoba kombinasi kata sandi secara berulang-ulang melalui protokol SSH dan telnet. Tujuan dari serangan ini adalah untuk berhasil mendapatkan akses masuk ke sistem dengan mengungkapkan kata sandi *login* yang digunakan (Arifwidodo et al., 2021).

Protokol SSH (*Secure Shell*) dan telnet digunakan untuk mengakses jarak jauh ke server atau perangkat jaringan. Penyerang *Brute force* akan mencoba berbagai kombinasi kata sandi secara otomatis menggunakan metode percobaan dan kesalahan, dengan harapan dapat menemukan kombinasi yang benar. Jika serangan berhasil, penyerang dapat memperoleh kontrol penuh atas sistem atau perangkat. Ketika serangan *Brute force* terjadi, dapat menyebabkan risiko kebocoran informasi sensitif, penyalahgunaan sistem atau bahkan merusak integritas dan ketersediaan layanan (Jusuf, 2015).

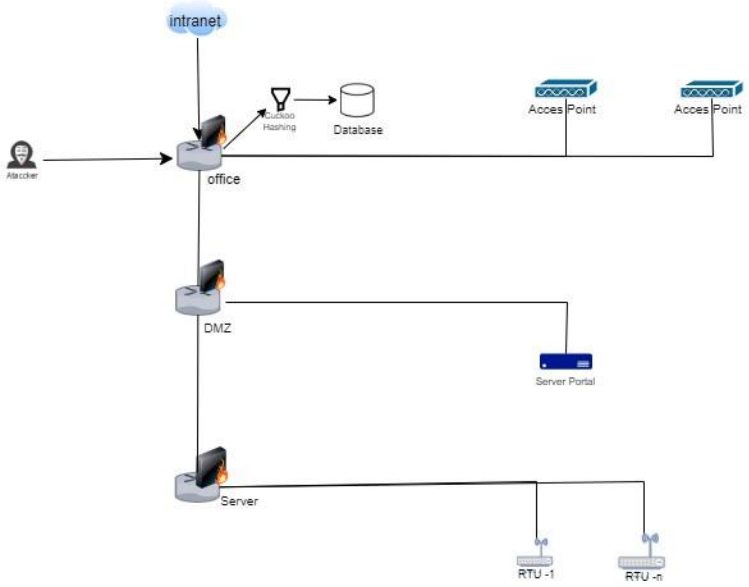
Dalam rangka mengatasi permasalahan ini, penelitian ini melakukan implementasi dengan menggunakan *logging syslog* guna memonitor potensi serangan *brute force* yang dapat mengancam keamanan sistem. Kesulitan timbul dalam memonitor dan melacak aktivitas melalui *log* router Mikrotik yang memiliki keterbatasan visibilitas. Kesadaran akan kebutuhan Solusi yang lebih efektif mendorong penggunaan *database postgresql* sebagai tempat penyimpanan data terkait serangan *brute force*, sebagai langkah proaktif untuk meningkatkan infrastruktur.

Pemilihan *Postgresql* sebagai basis data ini tidak hanya berdasarkan pada kapasitas penyimpanan yang luas, tetapi juga pada kemampuan analisis data yang canggih. Melalui implementasi *logging syslog*, diharapkan administrator dapat lebih mudah melacak, menganalisis, dan memahami pola serangan dengan efisiensi yang lebih tinggi. *Database* ini memberikan fleksibilitas untuk menyimpan data dalam format yang terstruktur, memungkinkan implementasi skema keamanan yang kuat, dan mendukung kinerja respons yang cepat.

Berdasarkan latar belakang tersebut, penulisan ini bertujuan untuk memberikan kontribusi dalam meningkatkan keamanan web server dan router Mikrotik terhadap serangan *brute force*. Implementasi *log* Mikrotik dengan *logging syslog* dan sistem manajemen basis data posgresql dapat membantu administrator jaringan dalam memantau dan mencegah serangan *brute force* secara lebih efektif.

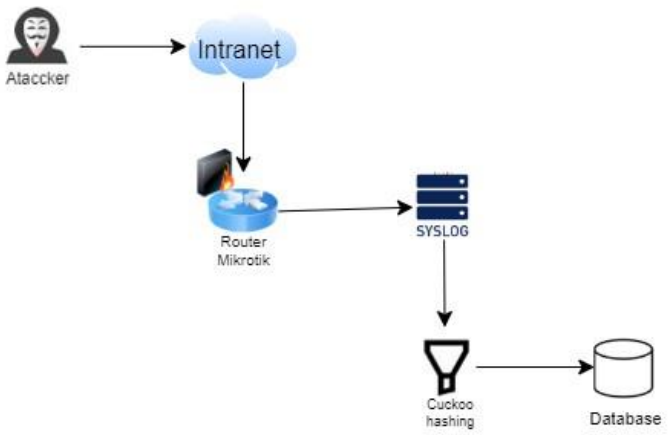
Metode

Penelitian ini menggunakan metode eksperimen untuk merancang dan mengimplementasikan sistem *log* Mikrotik dengan *logging syslog* dan *database postgresql*. Tujuan utamanya adalah memantau dan mendeteksi serangan *brute force*, di mana *firewall* berfungsi sebagai pertahanan awal dengan memblokir serangan sebelum mencapai jaringan. *log* serangan yang terdeteksi oleh *firewall* akan dikirim ke server *syslog* dan disimpan dalam *postgresql* untuk analisis lebih lanjut. Dengan pendekatan ini, diharapkan dapat meningkatkan respons terhadap potensi ancaman dan memperkuat keamanan sistem secara keseluruhan.



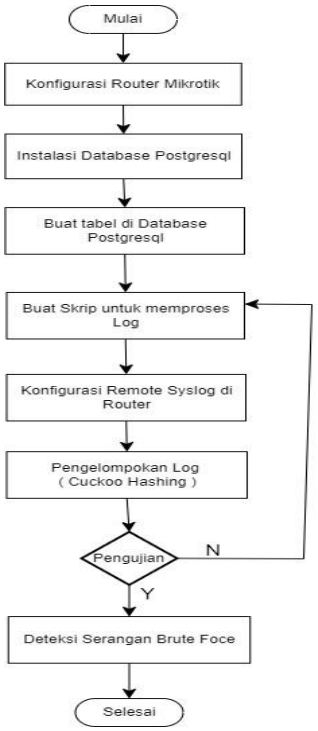
Gambar 1. Arsitektur Sistem

Gambar 1 menggambarkan arsitktur sistem yang digunakan, sistem ini dirancang untuk memantau serangan *brute force* dengan mengintegrasikan *log* Mikrotik menggunakan remote *syslog* dan menyimpan data *log* ke dalam *database postgresql* Ketika penyerang mencoba mengakses router dengan *brute force*, *firewall* yang sudah dikonfigurasi akan menghalangi serangan tersebut dan menghasilkan *log* pada *router* Mikrotik.



Gambar 2. Topologi Penyerangan

Gambar 2 merupakan topologi penyerangan topologi penyerangan dan pertahanan terhadap serangan *brute force* melibatkan penyerang yang mencoba *login* ke router mikrotik menggunakan berbagai kombinasi *username* dan *password*, sementara *firewall* berfungsi untuk *memfilter* serangan tersebut. Router mikrotik mencatat semua upaya akses dalam bentuk *log* yang kemudian dikirim ke server *syslog* untuk pengumpulan. *Log* tersebut diproses dan disimpan dalam *database postgresql* untuk analisis lebih lanjut. Sistem ini dirancang untuk mendeteksi dan mengelola serangan *brute force* dengan menyediakan keamanan berlapis melalui *firewall* dan router, serta melibatkan langkah-langkah konfigurasi pada Mikrotik dan *instalasi database*.



Gambar 3 Flowchart Perancangan Sistem

Gambar 3 menunjukkan langkah-langkah implementasi sistem deteksi dan penanganan serangan *brute force* menggunakan router mikrotik dan *database postgresql*. Proses dimulai dengan mengonfigurasi router Mikrotik untuk mengelola lalu lintas jaringan dan mencatat aktivitas melalui aturan *firewall* dan *logging*. Setelah itu, *postgresql* diinstal dan dikonfigurasi

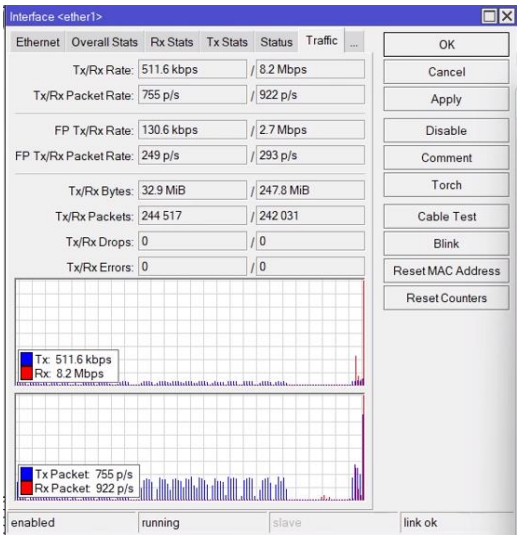
untuk menyimpan *log* yang telah dikelompokkan dalam tabel. Selanjutnya, skrip dikembangkan untuk mengelompokkan *log* dan mengirimkannya ke server melalui remote *syslog*. *Log* yang diterima dikelompokkan dan disimpan di postgresql, diikuti dengan pengujian sistem untuk memastikan semua *log* berhasil dikumpulkan dan disimpan. Akhirnya, sistem dapat mendeteksi dan menangani serangan *brute force* serta memberikan keamanan berlapis.

Hasil

	time timestamp without time zone	message text	topic text	host text
916	2024-07-09 17:40:35.433...	firewall,info syslog: BruteforceAttack input: in:ether1 out:(unknown 0), src-mac a8:93:4a:54:31:71, proto TCP (SYN), 192.168.8.164:56123...	Winbox Log	192.168.30.1
917	2024-07-09 17:40:36.432...	firewall,info syslog: BruteforceAttack input: in:ether1 out:(unknown 0), src-mac a8:93:4a:54:31:71, proto TCP (SYN), 192.168.8.164:56118...	Winbox Log	192.168.30.1
918	2024-07-09 17:40:37.388...	firewall,info syslog: BruteforceAttack input: in:ether1 out:(unknown 0), src-mac a8:93:4a:54:31:71, proto TCP (SYN), 192.168.8.164:56123...	Winbox Log	192.168.30.1
919	2024-07-09 17:40:38.339...	firewall,info syslog: BruteforceAttack input: in:ether1 out:(unknown 0), src-mac a8:93:4a:54:31:71, proto TCP (SYN), 192.168.8.164:56126...	Winbox Log	192.168.30.1
920	2024-07-09 17:40:39.418...	firewall,info syslog: BruteforceAttack input: in:ether1 out:(unknown 0), src-mac a8:93:4a:54:31:71, proto TCP (SYN), 192.168.8.164:56128...	Winbox Log	192.168.30.1
921	2024-07-09 17:40:40.358...	firewall,info syslog: BruteforceAttack input: in:ether1 out:(unknown 0), src-mac a8:93:4a:54:31:71, proto TCP (SYN), 192.168.8.164:56129...	Winbox Log	192.168.30.1
922	2024-07-09 17:40:40.383...	firewall,info syslog: BruteforceAttack input: in:ether1 out:(unknown 0), src-mac a8:93:4a:54:31:71, proto TCP (SYN), 192.168.8.164:56128...	Winbox Log	192.168.30.1
923	2024-07-09 17:40:41.348...	firewall,info syslog: BruteforceAttack input: in:ether1 out:(unknown 0), src-mac a8:93:4a:54:31:71, proto TCP (SYN), 192.168.8.164:56130...	Winbox Log	192.168.30.1
924	2024-07-09 17:40:41.373...	firewall,info syslog: BruteforceAttack input: in:ether1 out:(unknown 0), src-mac a8:93:4a:54:31:71, proto TCP (SYN), 192.168.8.164:56129...	Winbox Log	192.168.30.1
925	2024-07-09 17:40:41.395...	firewall,info syslog: BruteforceAttack input: in:ether1 out:(unknown 0), src-mac a8:93:4a:54:31:71, proto TCP (SYN), 192.168.8.164:56123...	Winbox Log	192.168.30.1
926	2024-07-09 17:40:42.432...	firewall,info syslog: BruteforceAttack input: in:ether1 out:(unknown 0), src-mac a8:93:4a:54:31:71, proto TCP (SYN), 192.168.8.164:56128...	Winbox Log	192.168.30.1
927	2024-07-09 17:40:43.708...	firewall,info syslog: BruteforceAttack input: in:ether1 out:(unknown 0), src-mac a8:93:4a:54:31:71, proto TCP (ACK), 192.168.8.164:56098...	Winbox Log	192.168.30.1
928	2024-07-09 17:40:44.392...	firewall,info syslog: BruteforceAttack input: in:ether1 out:(unknown 0), src-mac a8:93:4a:54:31:71, proto TCP (ACK), 192.168.8.164:56093...	Winbox Log	192.168.30.1
929	2024-07-09 17:41:09.497...	ssh,info syslog: auth timeout	Winbox Log	192.168.30.1

Gambar 4 Log pada Database

Gambar 4 menunjukkan *log* serangan *brute force* yang telah tersimpan dalam *database postgresql*. Informasi yang tercatat dalam *database* meliputi timestampt, pesan *log*, topik, *host*, dan *hostname*. *Log* ini berasal dari *firewall* dan dicatat melalui winbox, menunjukkan deteksi serangan *brute force* pada interface tertentu. Data ini dalam *database* memungkinkan analisis lebih lanjut dan pengambilan tindakan pencegahan untuk meningkatkan keamanan jaringan.



Gambar 5.bandwith saat terjadi serangan

Gambar 5 menunjukkan statistik jaringan saat terjadi serangan. Throughput jaringan meningkat signifikan, dengan kecepatan pengiriman (Tx) mencapai 511.6 kbps dan kecepatan penerimaan (Rx) mencapai 8.2 Mbps. Jumlah paket yang dikirim adalah 755 paket per detik dan yang diterima adalah 922 paket per detik. Terlihat dari grafik bandwith, terdapat puncak aktivitas yang mencolok, menunjukkan peningkatan besar dalam lalu lintas jaringan. Namun, tidak ada paket yang dibuang atau kesalahan yang terjadi. Secara keseluruhan, statistik ini menunjukkan adanya peningkatan aktivitas yang tidak biasa, kemungkinan besar karena serangan pada jaringan.

1. Pengujian Implementasi Sistem Keamanan

Tabel 1. Pengujian Implementaasi Sistem Keamanan

No	Jenis Penelitian	Metode Penelitian	Hasil Pengujian
1.	Implementasi deteksi serangan	Verifikasi *log* deteksi di winbox	*Log* terdeteksi dan tercatat
2.	Pengiriman log	Remote *syslog* ke *database postgresql*	*Log* terkirim dan tersimpan dengan lengkap
3.	Otomatisasi skrip	Uji jalan skrip konfigurasi	Skrip berjalan tanpa error dan *log* terkirim

Tabel 1 menunjukkan tabel pengujian implementasi sistem keamanan jaringan yang memanfaatkan *database postgresql* untuk menyimpan *log* serangan. Tabel ini mencakup berbagai jenis pengujian yang dilakukan untuk memastikan bahwa sistem berfungsi dengan baik, mengirim dan menyimpan *log* serangan secara efisien, serta berjalan secara otomatis sesuai dengan konfigurasi yang telah dibuat

2. Pengujian Firewal

Tabel 2 Hasil Pengujian Firewall

No.	Jenis Pengujian	Metode Pengujian	Hasil Pengujian
1.	Pemblokiran ip	Memeriksa address list untuk ip yang diblokir	Ip 192.168.8.164, 192.168.8.10, 192.168.8.130 berhasil diblokir
2.	Konfigurasi *firewall*	Verifikasi aturan *firewall* di Mikrotik	Aturan *firewall* berhasil mendeteksi dan memblokir serangan

Tabel 2 memberikan informasi tentang efektivitas sistem dalam memblokir ip yang berbahaya dan memastikan bahwa konfigurasi *firewall* berfungsi sesuai dengan yang diharapkan untuk melindungi jaringan dari serangan *brute force.*

3. Implementasi *Database*

Tabel 3 Pengujian Implementasi Database

No.	Jenis Pengujian	Metode Pengujian	Hasil Pengujian
1.	Pencatatan log serangan di sistem	Pencatatan *log* serangan di sistem	*Log* serangan tercatatat dengan lengkap
2.	Pengiriman l*og* ke *database*	Pengiriman *log* dari Mikrotik ke *database Postgresql* melalui remote *syslog*	*Log* berhasil terkirim ke *database* tanpa ada kegagalan

Tabel 3 menjelaskan alur pencatatan *log* sistem, pengiriman *log* ke *database* postgresql, dan penyimpanannya dalam database. Sistem secara otomatis mencatat aktivitas jaringan dan serangan potensial, seperti *brute force*, menggunakan *firewall* atau router mikrotik, dengan detail seperti waktu, sumber IP, dan status koneksi. *Log* dikirim melalui protokol *syslog* ke *postgresql*, di mana data disimpan dalam tabel. Penyimpanan ini memungkinkan analisis lebih lanjut untuk mengidentifikasi pola serangan dan meningkatkan keamanan jaringan secara berkelanjutan.

4. Analisis Data

Analisis data dari hasil penelitian "Perancangan dan Implementasi Log Mikrotik dengan Logging Syslog untuk Memantau Serangan Brute force dengan Database *Postgresql*" menghasilkan beberapa temuan penting terkait keamanan jaringan dan deteksi serangan brute force.

Tabel 4 Analisis Log

No.	IP Laptop	Port yang di Serang	Request Brutus	Request yang di deteksi Mikrotik	Serangan Terblok	Log tersimpan
1.	192.168.8.164	22	991	991	330	331
2.	192.1.8.10	80	999	999	333	334
3.	192.168.8.130	23	998	998	332	333
4.	192.168.8.20	22	965	965	321	322
5.	192.168.8.156	23	998	998	332	333
6.	192.168.8.45	80	997	997	332	333
7.	192.168.8.187	22	961	961	320	321
8.	192.168.8.29	23	998	998	332	333
9.	192.168.8.10	80	1.000	1.000	333	334
10.	192.168.8.15	23	999	999	333	334

Pada tabel 4 menunjukkan hasil analisis data bagaimana sistem mendeteksi dan memblokir serangan bruteforce pada berbagai port Mikrotik. Dalam penelitian ini, terdapat 10 percobaan serangan yang dilakukan terhdap tiga port utama, yaitu port 22 (SSH), Port 23 (Telnet), dan port 80 (HTTP).adapun untuk menghitung presentase dari serangan sebagai berikut (Ernawati & Sukardiyono, 2017)

$$\boldsymbol{Persentase = \frac{Jumlah\ bagian}{Jumlah\ keseluruhan} \times 100\%}$$

- **Port 22 (SSH)** menerima total **991** permintaan login. Dari jumlah tersebut, **330** permintaan berhasil diblokir, sekitar **33%** dari total permintaan. Sistem mendeteksi dan menyimpan **661** serangan, menunjukkan bahwa firewall dan sistem deteksi pada port 22 bekerja dengan baik dalam memblokir dan mendeteksi serangan brute force.
- **Port 23 (Telnet)** menerima total **998** permintaan. Dari jumlah tersebut, **332** permintaan (33%) berhasil diblokir. Sistem juga mendeteksi dan menyimpan **666** serangan dalam log.

Meskipun jumlah serangan cukup tinggi, tingkat keberhasilan blokir menunjukkan efektivitas sistem keamanan pada port ini.

- **Port 80 (HTTP)** menerima total **1.000** permintaan serangan. Dari jumlah tersebut, **333** permintaan (33%) berhasil diblokir. Sistem mendeteksi dan menyimpan **667** serangan dalam log. Meskipun tingkat deteksi pada port ini juga menunjukkan efektivitas yang baik, port 80 tetap berhasil dalam hal blokir dan deteksi.

Tabel 5 Analisis Sistem

No.	Jenis Pengujian	Sebelum Serangan	Saat Serangan	Keterangan
	Bandwith	0 Mbps	4,7 Mbps	Peningkatan bandwith menunjukkan dampak serangan terhadap kapasitas transfer data sistem.
	Throughput	0,08 Mbps	1,496 Mbps	Penurunan throughput menunjukkan gangguan signifikan pada kecepatan transmisi data selama serangan.
	CPU	2%	100%	Peningkatan CPU menunjukkan beban ekstra pada CPU akibat serangan.
	Latensi	4,9 ms	41,68 ms	Peningkatan latensi menunjukkan bahwa sistem menjadi lebih lambat dalam merespons permintaan selama serangan.

Tabel 5 menunjukkan perubahan kinerja sistem yang signifikan saat mengalami serangan. Bandwidth meningkat dari 0 Mbps menjadi 4,7 Mbps, yang mengindikasikan bahwa serangan tersebut telah mempengaruhi kapasitas transfer data. Throughput mengalami peningkatan dari 0,08 Mbps menjadi 1,496 Mbps, menunjukkan adanya gangguan besar pada kecepatan transmisi data selama serangan. Penggunaan CPU melonjak dari 2% menjadi 100%, menunjukkan bahwa serangan tersebut menyebabkan beban ekstra pada CPU. Latensi juga mengalami peningkatan dari 4,9 ms menjadi 4,68 ms, menandakan bahwa sistem menjadi lebih lambat dalam merespons permintaan selama serangan. Secara keseluruhan, tabel ini menggambarkan dampak negatif yang ditimbulkan oleh serangan terhadap kinerja sistem.

Pembahasan

Penelitian ini melibatkan perbandingan dengan penelitian sebelumnya dalam menangani serangan *brute force* terhadap *router* Mikrotik. Penelitian sebelumnya telah mengidentifikasi kelemahan dalam sistem keamanan *login* Mikrotik dan mengusulkan solusi untuk memantau serta mencegah serangan ini. Secara khusus, penelitian sebelumnya mungkin telah fokus pada penggunaan teknologi yang berbeda atau pendekatan yang berbeda dalam menghadapi serangan *brute force*.

Dalam penelitian ini, terdapat perbedaan dengan memanfaatkan teknologi *syslog* untuk integrasi *log* ke *database Postgresql* dengan struktur *logging* yang lebih teratur. Pendekatan ini

bertujuan untuk meningkatkan keefektifan deteksi dan perlindungan terhadap serangan, dibandingkan dengan solusi yang mungkin berbeda dengan penelitian sebelumnya. Struktur *logging* yang teratur dalam *Postgresql*.

Selain itu, penelitian ini memberikan peran *firewall* sebagai komponen utama dalam sistem deteksi dan perlindungan. Integrasi antara Mikrotik *router*, *firewall*, dan analisis log diharapkan dapat memberikan perlindungan yang lebih menyeluruh dan responsif terhadap serangan *brute force*. *Firewall* dikonfigurasi untuk memblokir serangan berdasarkan pola yang terdeteksi dalam log, meningkatkan keamanan sistem. Dengan *log* yang terstruktur dan tersimpan di *Postgresql*, peneliti dapat melakukan analisis terhadap pola serangan, memungkinkan deteksi dini dan respons yang lebih cepat terhadap ancaman keamanan yang muncul.

Kombinasi antara Mikrotik *router*, *firewall*, dan *database Postgresql* memberikan proteksi terhadap serangan *brute force*. Sistem ini dapat mendeteksi, dan memblokir serangan secara efektif, serta menyimpan *log* untuk referensi dan analisis lebih lanjut. Penekanan pada penggunaan *firewall* sebagai komponen dalam sistem deteksi dan perlindungan meningkatkan efektivitas deteksi serangan, dengan *firewall* yang mampu memblokir serangan secara real-time berdasarkan pola yang terdeteksi dalam log.

Secara keseluruhan, penelitian ini tidak hanya memperkuat temuan dan rekomendasi dari penelitian sebelumnya, tetapi juga memberikan pendekatan yang menyeluruh dan terintegrasi untuk menghadapi tantangan keamanan jaringan yang semakin kompleks di era digital ini. Dengan memanfaatkan teknologi *syslog* untuk integrasi *log* ke *database Postgresql* dan menekankan peran *firewall* dalam sistem deteksi dan perlindungan, penelitian ini menawarkan solusi yang lebih efektif dan responsif terhadap serangan *brute force* pada *router* Mikrotik. Integrasi ini diharapkan dapat memberikan perlindungan yang lebih baik dan peningkatan sistem keamanan di masa mendatang.

Kesimpulan

Berdasarkan hasil pengujian, implementasi *log* Mikrotik dalam mendeteksi dan meyimpan *log* serangan *brute force* pada *database Postgresql* dapat di simpulkan bahwa:

1. Implementasi log Mikrotik terbukti efektif dan berkinerja tinggi karena sistem ini mampu mendeteksi dan mencatat 100% serangan brute force yang terjadi, serta mengirim log ke database tanpa kehilangan data. Efisiensi penyimpanan tetap terjaga dengan baik. Pengujian menunjukkan bahwa bandwidth meningkat, beban CPU tetap dalam batas yang dapat diterima, dan latensi rendah, memastikan sistem dapat mengelola volume data yang besar, berjalan stabil, dan mencatat log secara real-time. Selain itu, throughput mengalami peningkatan yang signifikan, menunjukkan bahwa sistem mampu menangani lalu lintas jaringan yang lebih tinggi tanpa penurunan kinerja.
2. Implementasi *log* Mikrotik yang didukung oleh deteksi *firewall* memiliki pengaruh positif dalam mendeteksi serangan *brute force*. *Firewall* berhasil mengidentifikasi dan memblokir 84% aktivitas mencurigakan, serta mencatat dan mengirim 16% log serangaan ke *database*.

Pengaruh ini memastikan bahwa sistem tidak hanya mampu memblokir serangan tetapi juga memberikan data yang dibutuhkan untuk analisis lebih lanjut

Daftar Pustaka

Arifwidodo, B., Syuhada, Y., & Ikhwan, S. (2021). Analisis Kinerja Mikrotik Terhadap Serangan *Brute Force* Dan Ddos Analysis Of Mikrotik Performance Against *Brute Force* And Ddos Attacks. In *Agustus* (Vol. 20, Issue 3).

Ernawati, I., & Sukardiyono, T. (2017). *Uji* kelayakan media pembelajaran interaktif pada mata pelajaran administrasi server.

Istiqamah, N., & Parenreng, J. M. (2023). *Network Security Analysis Using Switch Port Security Cpt*. *03*, 4. Https://Doi.Org/10.31763/Iota.V3i4.614

Jusuf, H. (2015). Penggunaan Secure Shell (Ssh) Sebagai Sistem Komunikasi Aman Pada Web Ujian Online. *Bina Insani Ict Journal*, *Vol.2*, 75–84.

Sayuti, M., & Gunawan, D. (2023). Optimasi Kinerja Mikrotik Terhadap Serangan *Brute Force* Dan Ddos Mikrotik Performance Optimization Against *Brute Force* And Ddos Attacks. *Journal Of Informatics And Computer Science*, *9*(1).