Jurnal Infortech
Volume 6 No. 1 Juni 2024
E-ISSN: 2715-8160

Perancangan Keamanan Router Mikrotik Dari Serangan FTP Dan SSH Brute Force

Ahmad Fauzi[1*], Firmansyah[2], Tommi Alfian Armawan Sandi[3]

[1]Sistem Informasi, Fakultas Teknologi Informasi, Universitas Nusa Mandiri, Jakarta
e-mail: [1]ahmad.azy@nusamandiri.ac.id
[2,3]Informatika, Fakultas Teknik dan Informatika, Universitas Bina Sarana Informatika, Jakarta
e-mail: [2]firmansyah.fmy@bsi.ac.id, [3]tommi.taf@bsi.ac.id

Diterima	Direvisi	Disetujui
27-02-2024	03-05-2024	05-06-2024

Abstrak - Keamanan jaringan merupakan aspek kritis dalam memastikan integritas dan kerahasiaan data dalam suatu sistem. Router MikroTik, yang sering digunakan dalam jaringan kecil hingga menengah, juga memerlukan perhatian khusus terkait keamanan untuk melindungi informasi yang melintas melalui perangkat tersebut. Salah satu ancaman umum adalah serangan *Brute Force* pada protokol FTP (*File Transfer Protocol*) dan SSH (*Secure Shell*). Penelitian ini fokus pada pengembangan dan peningkatan keamanan router MikroTik melalui identifikasi, deteksi, dan mitigasi serangan *Brute Force* pada FTP dan SSH. Metode analisis log yang canggih dan implementasi algoritma deteksi serangan yang efisien digunakan untuk memantau aktivitas yang mencurigakan. Selain itu, solusi pengamanan seperti pembatasan percobaan login, implementasi CAPTCHA, dan manajemen akses yang lebih ketat diterapkan untuk memitigasi risiko serangan. Eksperimen dilakukan untuk mengevaluasi efektivitas metode yang diusulkan dalam mengurangi insiden serangan *Brute Force*. Hasilnya menunjukkan peningkatan yang signifikan dalam mendeteksi dan mengatasi serangan, sehingga meningkatkan keamanan router MikroTik dari ancaman yang bersifat persisten dan terus berkembang. Penelitian ini memberikan kontribusi pada pemahaman lebih lanjut tentang taktik serangan *Brute Force* pada router MikroTik dan memberikan solusi praktis untuk memperkuat pertahanan keamanan jaringan. Dengan menerapkan langkah-langkah keamanan yang disarankan, organisasi dapat meningkatkan ketahanan jaringan mereka terhadap serangan potensial dan melindungi integritas data mereka.

Kata kunci: Keamanan jaringan, FTP *Brute Force*, SSH *Brute Force*

Abstract *- Network security is a critical aspect in ensuring the integrity and confidentiality of data in a system. MikroTik routers, which are often used in small to medium networks, also require special attention regarding security to protect the information that passes through the device. One common threat is Brute Force attacks on the FTP (File Transfer Protocol) and SSH (Secure Shell) protocols. This research focuses on developing and improving the security of MikroTik routers through identification, detection and mitigation of Brute Force attacks on FTP and SSH. Sophisticated log analysis methods and implementation of efficient attack detection algorithms are used to monitor suspicious activity. In addition, security solutions such as limiting login attempts, CAPTCHA implementation, and stricter access management were implemented to mitigate the risk of attacks. Experiments were conducted to evaluate the effectiveness of the proposed method in reducing the incidence of Brute Force attacks. The results show significant improvements in detecting and resolving attacks, thereby increasing the security of MikroTik routers from persistent and evolving threats. This research contributes to further understanding of Brute Force attack tactics on MikroTik routers and provides practical solutions to strengthen network security defenses . By implementing recommended security measures, organizations can increase the resilience of their networks to potential attacks and protect the integrity of their data.*

Keywords: Network security, FTP Brute Force, SSH Brute Force

PENDAHULUAN

Dalam era digital yang terus berkembang pesat, keamanan jaringan menjadi prioritas utama bagi organisasi dan individu yang mengandalkan konektivitas untuk berbagai keperluan (Marlinda et al., 2019) . Penelitian yang dilakukan dengan membentuk jaringan LAN berdasarkan skema yang sudah dibuat dengan pengguaan perangkat Router secara mandiri sehingaa sebelum adanya keamanan pada protokol FTP dan SSH maka Router melayani setiap permintaan login walau dengan user dan password yang salah yang dapat terlihat dari Log Hisotynya sehingga seseorang tanpa batas kesalahan

login dapat mncoba-coba masuk kedalam sistem Mikrotik dengan menebak-nebak user dan password dengan demikian fitur untuk membatasi user yang ingin mencoba-coba login dengan user dan password yang salah perlu adanya batasan untuk menghidari percobaan masuk kedalam sistem mikrotik, Router MikroTik, sebagai salah satu komponen inti dalam infrastruktur jaringan, memiliki peran sentral dalam mengamankan aliran data yang melintasinya. Namun, dalam menghadapi ancaman serangan yang semakin kompleks, khususnya melalui protokol FTP (*File Transfer Protocol*) dan SSH (*Secure Shell*), diperlukan upaya lebih lanjut untuk meningkatkan keamanan router MikroTik (Fauzi et al., 2022). Serangan *Brute Force* pada protokol FTP dan SSH telah menjadi ancaman serius terhadap keamanan jaringan. Pendekatan ini melibatkan upaya berulang untuk menebak kombinasi kata sandi hingga berhasil masuk ke dalam sistem. Router MikroTik, sebagai titik masuk penting ke dalam jaringan, rentan terhadap serangan semacam ini. Keberhasilan serangan *Brute Force* dapat menyebabkan pencurian informasi sensitif, gangguan layanan, dan bahkan akses tak sah ke dalam jaringan. Tujuan utama penelitian ini adalah meningkatkan keamanan jaringan router MikroTik dari serangan FTP dan SSH *Brute Force* (Madcoms, 2019). Dengan mendalaminya, penelitian ini bertujuan untuk mengidentifikasi potensi celah keamanan, mengembangkan metode deteksi yang efektif, dan menerapkan solusi yang dapat memitigasi risiko serangan dengan efisien. Penelitian ini menggunakan pendekatan gabungan antara analisis log, pengembangan algoritma deteksi serangan, dan implementasi langkah-langkah keamanan yang cermat pada router MikroTik. Pengumpulan data dilakukan melalui pemantauan aktivitas jaringan yang dirancang jaringan pribadi atau internal berdasarkan skema yang sudah di rancang, dan eksperimen dilakukan untuk mengevaluasi keefektifan solusi yang diusulkan. Metode penelitian ini diharapkan dapat memberikan wawasan mendalam tentang cara melindungi router MikroTik dari serangan *Brute Force* pada protokol FTP dan SSH. Dengan merinci latar belakang, tujuan, dan metode penelitian, penelitian ini diarahkan untuk memberikan kontribusi yang signifikan terhadap pengembangan strategi keamanan jaringan yang tangguh dan efektif, khususnya dalam menghadapi ancaman *Brute Force* pada router MikroTik (Tommi Alfian Armawan Sandi et al., 2022).

METODE PENELITIAN

Penelitian ini akan mengadopsi pendekatan gabungan antara analisis log, pengembangan algoritma deteksi serangan, dan implementasi langkah-langkah keamanan pada router MikroTik. Berikut adalah rincian lebih lanjut mengenai metode penelitian yang akan diterapkan:

1. Analisis Log Pemantauan aktivitas jaringan pada router MikroTik untuk mencatat pola lalu lintas yang mencurigakan, Analisis log secara mendalam untuk mengidentifikasi serangan *Brute Force* melalui protokol FTP dan SSH (Dewi & Firmansyah, 2019)
2. Pengembangan Algoritma Deteksi Serangan. Perancangan algoritma deteksi yang canggih untuk mengenali pola serangan *Brute Force*, Penggunaan teknik machine learning atau pendekatan kecerdasan buatan untuk meningkatkan kemampuan deteksi (Firmansyah et al., 2021)
3. Implementasi Langkah-Langkah Keamanan Pembatasan percobaan login: Menerapkan kebijakan yang membatasi jumlah percobaan login untuk mencegah serangan *Brute Force*, CAPTCHA: Menggunakan teknologi CAPTCHA untuk memverifikasi keaslian pengguna dan mencegah otomatisasi serangan (Wahyudi & Firmansyah, 2021)
4. Pengumpulan Data Pemantauan berkelanjutan terhadap aktivitas jaringan selama periode waktu yang cukup untuk mencakup berbagai situasi dan skenario serangan.
5. Eksperimen dan Evaluasi Implementasi solusi keamanan yang diusulkan pada lingkungan uji coba, Pengujian dan evaluasi kinerja sistem terhadap serangan *Brute Force* secara simulative (Indrianingsih et al., 2021).
6. Analisis Hasil
   Evaluasi hasil eksperimen untuk mengukur efektivitas langkah-langkah keamanan yang diimplementasikan, Identifikasi dan dokumentasi kelemahan atau area perbaikan potensial.

HASIL DAN PEMBAHASAN

FTP (*File Transfer Protocol*) *Brute Force* adalah metode serangan di mana penyerang mencoba secara berulang-ulang untuk mendapatkan akses ke sistem FTP dengan mencoba berbagai kombinasi nama pengguna dan kata sandi. FTP adalah protokol yang digunakan untuk mentransfer file antara perangkat dalam suatu jaringan. Serangan *Brute Force* pada protokol FTP dapat memberikan akses yang tidak sah ke sistem, memungkinkan penyerang untuk mengambil alih kontrol atas file atau mengungkapkan informasi sensitif yang disimpan dalam server FTP (Mugi Raharjo, Frengki Pernando, 2019).

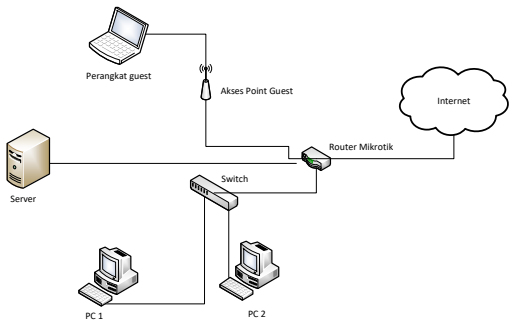
SSH (*Secure Shell*) *Brute Force* adalah metode serangan di mana penyerang mencoba secara berulang-ulang untuk mendapatkan akses ke sistem melalui protokol SSH dengan mencoba berbagai kombinasi nama pengguna dan kata sandi. SSH digunakan untuk mengamankan koneksi jaringan dan memberikan akses aman ke mesin jarak jauh. Serangan *Brute Force* pada protokol SSH bertujuan untuk mendapatkan akses yang tidak sah ke server

atau sistem terkait (Jamalul'ain & Nurdiawan, 2022).

Berikut adalah langkah-langkah umum yang dilibatkan dalam serangan FTP dan SSH *Brute Force*:

1. Identifikasi Target
   Penyerang mengidentifikasi server FTP/SSH yang menjadi target. Hal ini dapat dilakukan dengan melakukan pemindaian jaringan atau dengan mencari informasi terbuka tentang infrastruktur yang terhubung ke internet.
2. Pencarian Nama Pengguna
   Penyerang mencoba mengumpulkan informasi tentang nama pengguna yang valid di server FTP/SSH target. Ini bisa melibatkan pencarian publik, sosial engineering, atau penggunaan teknik lainnya untuk mengidentifikasi nama pengguna yang mungkin digunakan.
3. Pelaksanaan *Brute Force*
   Menggunakan skrip otomatis atau alat khusus, penyerang melakukan percobaan login otomatis dengan mencoba berbagai kombinasi nama pengguna dan kata sandi secara berurutan. Proses ini dapat dilakukan secara cepat dan terus menerus.
4. Deteksi Kesuksesan
   Penyerang memantau apakah kombinasi nama pengguna dan kata sandi tertentu berhasil memberikan akses ke server FTP/SSH. Begitu sukses, penyerang dapat memiliki kontrol penuh terhadap file yang ada di dalamnya.
5. Eksploitasi Akses
   Setelah mendapatkan akses, penyerang dapat menggunakan hak akses yang diperoleh untuk melakukan tindakan jahat, seperti mengunggah, mengunduh, menghapus, atau merusak file.

Berikut skema jaringan yang digunakan untuk penerapan keamanan jaringan router mikrotik dari serangan FTP dan SSH *Brute Force*.



Sumber : Hasil Penelitian 2024

Gambar 1. Skema jaringan Komputer

Pada gambar diatas merupakan sebuah topologi yang digunakan sebagai bahan penelitian yang dimana terdapat akses umum berupa perangkat akses point yang digunakan sebagai akses bagi para tamu yang disediakan agar dapat mengakses internet dan tidak hanya itu siapa saja bahkan dapat menjadi celah keamanan baik dari sisi internal atau external oleh sebab itu tidak dapat di pungkiri bahwasannya keamanan baiknya dilakukan dari segala penjuru akses router baik oleh akses point atau PC1 dan PC2

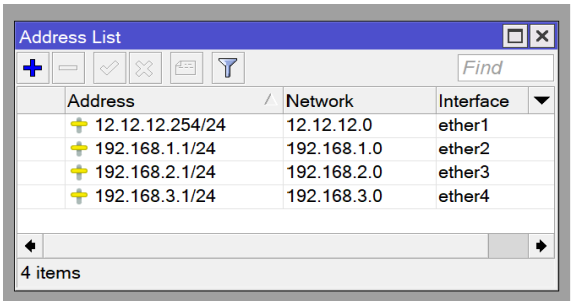
Berikut adalah pengalamatan IP pada Topologi tersebut.

Tabel 1. Mapping IP Address

Nama Perangkat	Interface	IP Address	Gatway
Router	Eth1	12.12.12.254/24	-
	Eth 2	192.168.1.1/24	-
	Eth 3	192.168.2.1/24	-
	Eth 4	192.168.3.1/24	-
Akses Point	WAN	192.168.1.254/24	192.168.1.1
	LAN	172.16.40.1/24	-
Server	NIC	192.168.2.10/24	192.168.2.1
PC1	NIC	192.168.3.10/24	192.168.3.1
PC2	NIC	192.168.3.11/24	

Sumber : Hasil Penelitian 2024

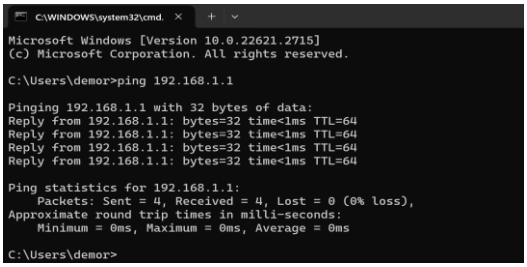
Pada perangkat Router merupakan sebuah perangkat yang digunakan untuk menghubungkan jaringan local dengan jaringan internet dengan menggunakan ether 2,3 dan 4 untuk akses jaringan local dan ether 1 yang digunakan untuk akses jaringan ISP/Internet.



Sumber : Hasil Penelitian 2024

Gambar 2. Konfigurasi IP address pada Router

Ip address yang sudah terdaftar pada address list merupakan sebuah pengaplikasian pada Mapping Ip address yang yang dibuat sebelumnya sehingga dapat mengkoneksikan antara Router dan client yang berada pada jaringan LAN.



Sumber : Hasil Penelitian 2024

Gambar 3. ICMP dari client menuju Router Mikrotik

Untuk memastikan semua perangkat dapat terkoneksi pada perangkat Router maka dilakukan ICMP masing-masing client menuju router agar memastikan clinet sudah dapat mengakses ke jaringan router berikut hasil rekapan dari hasil ICMP Client menuju Router:

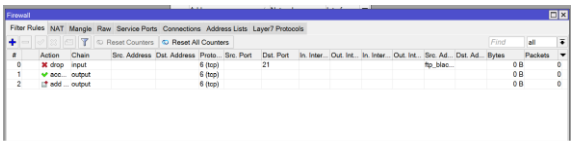
Tabel 2. Status ICMP dari Client menuju Router

Nama Cliet	IP Tujuan ICMP	Status
PC1	192.168.3.1	Connect
PC2	192.168.3.1	Connect
Server	192.168.2.1	Connect
Guest	172.16.40.1	Connect

Sumber : Hasil Penelitian 2024

Dengan berhasilnya proses ICMP dari clinet menuju Router maka dapat dipastikan sudah terjalinnya komunikasi jadingan antara Router dan Client sehingga tingat keamanan yang akan diterapkan adalah sebagai berikut:

/ip firewall filter
add chain=input protocol=tcp dst-port=21 src-address-list=ftp_blacklist action=drop comment="drop ftp *Brute Force*rs"
add chain=output action=accept protocol=tcp content="530 Login incorrect" dst-limit=1/1m,9,dst-address/1m
add chain=output action=add-dst-to-address-list protocol=tcp content="530 Login incorrect" address-list=ftp_blacklist address-list-timeout=3h

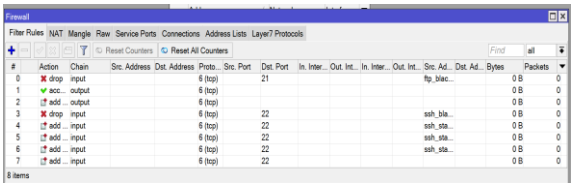


Sumber : Hasil Penelitian 2024

Gambar 4. Hasil Konfigurasi Mengamankan FTP dari serangan Bruteforce

Setelah konfigurasi untuk FTP sudah dibuatkan rantainya maka ketika ada user yang mencoba login FTP ke router lebih dari 10 kali gagal, maka IP Address dari user tersebut akan di drop selama 3 jam. Konfigurasi dapat Anda sesuikan sesuai dengan kebutuhan.

add chain=input protocol=tcp dst-port=22 src-address-list=ssh_blacklist action=drop comment="drop ssh *Brute Force*rs" disabled=no
add chain=input protocol=tcp dst-port=22 connection-state=new src-address-list=ssh_stage3 action=add-src-to-address-list address-list=ssh_blacklist address-list-timeout=10d comment="" disabled=no
add chain=input protocol=tcp dst-port=22 connection-state=new src-address-list=ssh_stage2 action=add-src-to-address-list address-list=ssh_stage3 address-list-timeout=1m comment="" disabled=no
add chain=input protocol=tcp dst-port=22 connection-state=new src-address-list=ssh_stage1 action=add-src-to-address-list address-list=ssh_stage2 address-list-timeout=1m comment="" disabled=no
add chain=input protocol=tcp dst-port=22 connection-state=new action=add-src-to-address-list address-list=ssh_stage1 address-list-timeout=1m comment="" disabled=no

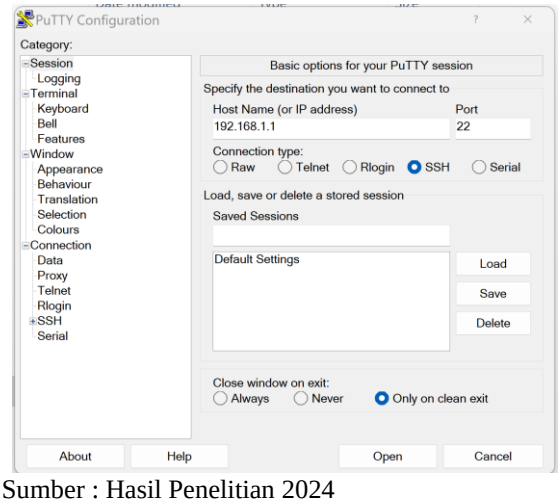


Sumber : Hasil Penelitian 2024

Gambar 5. Hasil Konfigurasi Mengamankan FTP dan SSH dari serangan Bruteforce

Dengan konfigurasi diatas, maka ketika ada client yang mencoba meremote Router melalui SSH dan mengalami gagal login selama lebih dari 3 kali, maka alamat IP penyerang akan di drop selama 10 Hari. Konfigurasi dapat Anda sesuaikan sesuai dengan kebutuhan.

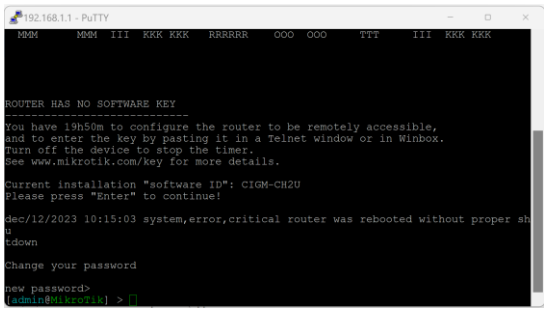
Pengujian dilakukan dengan menggunakan aplikasi Putty yang digunakan untuk meremote dan mengakses Router dengan melakukan percobaan pada port 21 TCP dan Port 22 SSH berikut hasil pengujian yang dilakukan dalam memasukan user dan password berkali-kali secara random/*Brute Force*.



Sumber : Hasil Penelitian 2024

Gambar 6. Aplikasi Putty

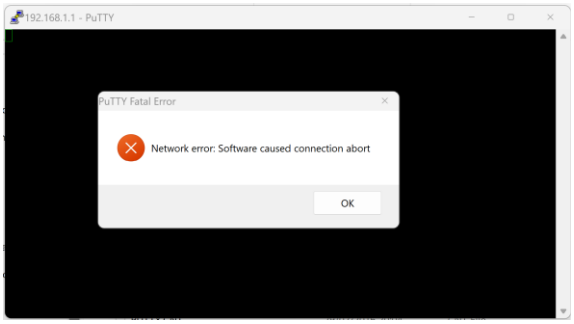
Dengan ditambahkannnya Chain fairwall maka terdapat perbedaan untuk keamanan Router Dimana bila diakses oleh user yang memiliki akun maka dapat di remote dengan dengan menggunakan aplikasi putty dengan tampilan sebagai berikut.



Sumber : Hasil Penelitian 2024

Gambar 7. Aplikasi Putty Diakses oleh User yang valid

Akan tetapi bila ada user yang mencoba menebak-nebak user dan password kedalam Router mikrotik dengan menggunakan aplikasi Putty maka dalam percobaan ke 10 akan di Drop dan tidak dapat mengakses Router Mikrotik dengan tampilan Putty sebagai berikut.



Sumber : Hasil Penelitian 2024

Gambar 8. Aplikasi Putty di Drop oleh Router

IP address yang digunakan untuk melakukan serangan brute forse telah di filter dan di drop untuk sementara waktu dikarenakan adanya Upaya dalam melakukan login secara acak.

Dengan demikian dengan adanya filter firewall ini dapat mencegah sesorang yang dengan sengaja ingin melakukan penyerangan kepada router dengan berbagai macam tujuan dan yang pasti aktifitas tersebut sudah melanggar karena orang tersebut bukanlah seorang yang berhak mengakses sebuah router.

KESIMPULAN

Secara default router Mikrotik merupakan sebuah perangkat yang digunakan untuk menghubungkan antar dua network yang berbeda, antara jaringan local area network dan jaringan internet sehingga seiring dengan perubahan jaman makan Router dapat menjadikan sebuah media Informasi untuk orang-orang yang tidak bertanggung jawab dengan mencoba memasuk kedalam system router dengan berbagai macam kebutuhan sehingga seorang yang melakukan aktifitas tersebut menjadi ancaman bagi system network yang sudah di rancang oleh sebuah istansi yang diberi kewenangan, dengan menggunakan metode STP dan SSH *Brute Force* memungkinkan seseorang dapat melakukan percobaan untuk dapat memasuki sebuah akses Router maka dengan adanya Firewall Chain yang di susun sedemikian rupa minimal dapat mencegah seseorang dalam mencoba melakukan akses kedalam Router, Dalam menghadapi ancaman serangan *Brute Force* pada protokol FTP dan SSH, penelitian ini berhasil menyajikan solusi proaktif dan efektif untuk meningkatkan keamanan jaringan pada router MikroTik. Analisis mendalam terhadap log aktivitas, pengembangan algoritma deteksi serangan yang canggih, dan implementasi langkah-langkah keamanan telah membuktikan dampak positifnya dalam memitigasi risiko serangan yang dapat menyebabkan kerugian dan kerentanan terhadap keamanan informasi.Melalui eksperimen yang dilakukan, solusi keamanan yang diusulkan berhasil mendeteksi dengan cepat dan mengatasi serangan *Brute Force*, mencegah akses yang tidak sah ke router MikroTik. Pembatasan percobaan login, penggunaan CAPTCHA, dan manajemen akses yang lebih ketat membuktikan efektivitasnya dalam mengurangi tingkat keberhasilan serangan *Brute Force*.Hasil penelitian ini memberikan pandangan yang lebih mendalam tentang cara melindungi router MikroTik dari serangan *Brute Force* pada protokol FTP dan SSH. Dengan menerapkan metode deteksi yang canggih dan langkah-langkah keamanan yang disarankan, organisasi dapat meminimalkan risiko kebocoran informasi, gangguan layanan, dan pengambilalihan kontrol yang tidak sah.Kesimpulannya, pengembangan keamanan jaringan pada router MikroTik dari serangan FTP dan SSH *Brute Force* tidak hanya esensial tetapi juga memungkinkan organisasi untuk menjaga integritas dan kerahasiaan data mereka. Keamanan yang ditingkatkan pada tingkat ini menjadi kunci dalam menghadapi ancaman keamanan yang terus berkembang, memberikan fondasi yang kuat untuk kelangsungan dan keberlanjutan operasional suatu jaringan.

REFERENSI

Dewi, S., & Firmansyah, F. (2019). Quality of Service Gateway Load Balancing Protocol Message Digest algorithm 5 Authentication For Network Quality Enhancement. *Journal of Telematics and Informatics*, *7*(1), 45–50. http://section.iaesonline.com/index.php/JTI/article/view/709

Fauzi, A., Firmansyah, F., & Nuriya, L. (2022). Workshop Manajemen Bandwidth Jaringan Komputer RT/RW pada Mitra Knowledge Connecting Community Kota Bekasi. *Jurnal Abdi Masyarakat Indonesia*, *3*(1), 163–170.

https://doi.org/10.54082/jamsi.600

Firmansyah, F., Purnama, R. A., Anton, A., & Astuti, R. D. (2021). Performa Redundancy Link Hot Standby Router Protocol IPv6 With Routing EIGRP for IPv6. *Jurnal Sains Dan Informatika*, *7*(1), 58–66. https://doi.org/10.34128/jsi.v7i1.297

Indrianingsih, Y., Wintolo, H., & Saputri, E. Y. (2021). Spanning Tree Protocol (STP) Based Computer Network Performance Analysis on BPDU Config Attacks and Take Over Root Bridge Using the Linear Regression Method. *Jurnal Online Informatika*, *6*(2), 155. https://doi.org/10.15575/join.v6i2.703

Jamalul'ain, A., & Nurdiawan, O. (2022). OPTIMALISASI KEAMANAN JARINGAN KOMPUTER MENGGUNAKAN METODE KNOCKING PORT BERBASIS MIKROTIK (Studi Kasus: CV. Mitra Indexindo Pratama). *Jurnal Mahasiswa Teknik Informatika)*, *6*(2), 560–570.

Madcoms. (2019). *Panduan Lengkap Membangun Sistem Jaringan Komputer Dengan Mikrotik RouterOS* (Madcoms (ed.); 1st ed.). Penerbit Andi.

Marlinda, L., Hermawan, A., & Fauzi, A. (2019). Sistem Informasi Pengelolaan Masjid Online Menggunakan Metode Waterfall. *Edik Informatika*, *6*(1), 20–27. https://doi.org/10.22202/ei.2019.v6i1.3634

Mugi Raharjo, Frengki Pernando, A. F. (2019). Perancangan Performansi Quality Of Service Dengan Metode Virtual Routing Redudancy Protocol (VRRP). *Teknik Komputer*, *V*(1), 87–92. https://doi.org/10.31294/jtk.v5i1.4555

Tommi Alfian Armawan Sandi, Firmansyah, F., Dewi, S., Pratama, E. K., & Astuti, R. D. (2022). Comparison of Port Security Switch Layer 2 MAC Address Dynamic With MAC Address Static Sticky. *Inspiration: Jurnal Teknologi Informasi Dan Komunikasi*, *12*(2), 65–75. https://doi.org/10.35585/inspir.v12i2.8

Wahyudi, M., & Firmansyah. (2021). Network Performance Optimization using Dynamic Enhanced Interior Routing Protocols Gateway Routing Protocol for IPv6 (EIGRPv6) and IPv6 Access Control List. *Journal of Physics: Conference Series*, *1830*(1). https://doi.org/10.1088/1742-6596/1830/1/012017