INSANtek – Jurnal Inovasi dan Sains Teknik Elektro
Volume 5 No. 2 November 2024
E-ISSN: 2722-547X

Penetration Testing Pada Sistem Keamanan Jaringan Dengan Metode Filtering Addresslist dan IPService

Mugi Raharjo[1], Firmansyah[2], Sri Watmah[3], Tommi Alfian Armawan Sandi[4], Jordy Lasmana Putra[5]

[1,5]Universitas Nusa Mandiri
e-mail: [1]mugi.mou@nusamandiri.ac.id, [1]jordy.jlp@nusamandiri.ac.id

[2,3,4]Universitas Bina Sarana informatika
e-mail: firmansyah.fmy@bsi.ac.id, sriwatmah.wtm@bsi.ac.id, tommi.taf@bsi.ac.id

Abstrak - Serangan *brute force* merupakan ancaman yang serius terhadap keamanan jaringan, terutama pada sistem autentikasi yang rentan seperti *password*. Penelitian ini bertujuan untuk mengatasi masalah tersebut dengan mengusulkan metode *filtering addresslist* menggunakan perangkat *Mikrotik* untuk mencegah serangan *brute force*. Kami melakukan penetrasi terhadap sistem jaringan yang telah ada untuk diuji kekuatan pertahananya dan kemudian mencari solusinya. Pendekatan ini melibatkan identifikasi alamat *IP* yang mencurigakan berdasarkan pola serangan *brute force*, kemudian memblokirnya menggunakan fitur *filtering addresslist* pada *router Mikrotik*. Penelitian ini dilakukan dengan mengumpulkan data serangan *brute force* dari jaringan uji, menganalisis pola serangan, dan mengimplementasikan metode *filtering addresslist*. Hasil eksperimen menunjukkan bahwa metode ini efektif mengurangi tingkat serangan *brute force* dalam jaringan, meningkatkan keamanan secara signifikan. Penelitian ini telah mengahasilkan uji penetrasi terhadap sistem keamanan dan kami telah menemukan celah-celah keamanan mana saja yang rentan terkena serangan, untuk itu telah diterapkan pengamanan lewat metode addreslist dan ip service untuk memblokir seranagn tersebut. Sehingga memberikan keamanan untuk sistem keamanan jaringan.

Kata Kunci: Keamanan Jaringan, *Brute Force*, Penyerangan

Abstract *- Brute force attacks are a serious threat to network security, especially in vulnerable authentication systems such as passwords. This study aims to overcome this problem by proposing a filtering addresslist method using Mikrotik devices to prevent brute force attacks. We penetrated the existing network system to test its defense strength and then find a solution. This approach involves identifying suspicious IP addresses based on brute force attack patterns, then blocking them using the filtering addresslist feature on the Mikrotik router. This study was conducted by collecting brute force attack data from the test network, analyzing attack patterns, and implementing the filtering addresslist method. The experimental results show that this method is effective in reducing the level of brute force attacks in the network, significantly increasing security. This study has produced a penetration test of the security system and we have found which security gaps are vulnerable to attack, for which security has been implemented through the addresslist method and ip services to block these attacks. Thus providing security for the network security system.*

Keywords*: Network Security, Brute Force, Attack*

PENDAHULUAN

Menanggapi meningkatnya ancaman yang ditimbulkan oleh serangan *brute force*, berbagai strategi mitigasi telah diusulkan dan diimplementasikan. Salah satu pendekatan tersebut melibatkan penggunaan *filtering address list*, yang bertujuan untuk mengidentifikasi dan memblokir alamat IP yang mencurigakan yang dikenal terkait dengan aktivitas serangan *brute force*. Router Mikrotik, yang banyak digunakan dalam infrastruktur jaringan, menawarkan fitur yang dapat dimanfaatkan untuk mengimplementasikan mekanisme *filtering* tersebut secara efektif.

Studi ini membangun pada penelitian yang telah ada dalam bidang keamanan jaringan dan bertujuan untuk menyelidiki efektivitas penggunaan router Mikrotik untuk mencegah serangan *brute force* melalui *filtering address list*. Dengan menganalisis pola serangan dan mengimplementasikan langkah-langkah proaktif, penelitian ini bertujuan untuk meningkatkan posisi keamanan sistem jaringan dan mengurangi risiko yang terkait dengan serangan *brute force*. Oleh karena itu keamanan dan kerahasiaan data pada jaringan komputer saat ini menjadi isu yang sangat penting dan terus berkembang (Dewi & Islami, 2021).

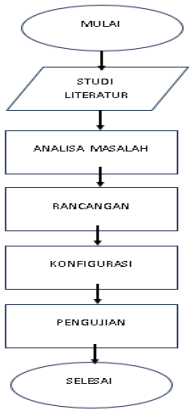
Komputer sebagai salah satu bentuk teknologi yang sedang berkembang pesat saat ini mempunyai peranan yang sangat penting bagi manusia. Dengan adanya komputer pekerjaan manusia menjadi lebih mudah (Watmah, 2022). Berkembangnya teknologi yang semakin cepat membuat keamanan jaringan perlu diperhatikan. Keamanan jaringan komputer merupakan bagian yang sangat penting dalam suatu sistem .(Cahya, Rizki, Sutiyo, Saputra, & Elfarizi, 2023) Keamanan siber merupakan bidang yang berkaitan dengan melindungi sistem komputer, jaringan, dan data dari ancaman dan serangan yang dilakukan secara elektronik. Ancaman-ancaman dalam dunia maya dapat berasal dari berbagai pihak seperti *hacker*, *malware*, *phishing* dan masih banyak lagi. (Shafiyyah, Elektro, Teknik, & Lampung, 2024) Keamanan Jaringan merupakan salah sat aspek terpenting dalam sebuah jaringan. Akan tetapi seringkali masalah keamanan jaringan dipandang sebelah mata (Desmira & Wiryadinata, 2022)

MikroTik sekarang menyediakan *hardware* dan *software* untuk konektivitas internet di sebagian besar negara di seluruh dunia. Produk hardware unggulan Mikrotik berupa *Router*, *Switch*, Antena, dan perangkat pendukung lainnya. Sedangkan produk *Software* unggulan Mikrotik adalah Mikrotik *RouterOS* (Jawad,Amalia,Nadzarudien , 2023) *Firewall* didefinisikan sebagai suatu cara atau mekanisme yang diterapkan baik terhadap hardware, *software* ataupun sistem itu sendiri dengan tujuan untuk melindungi, baik dengan menyaring, membatasi atau bahkan menolak suatu atau semua hubungan/kegiatan. (Yudi mulyanto, M. Julkarnain, & Jabi Afahar, 2021) Dengan ancaman siber yang terus berkembang, pendekatan preventif seperti pengaturan akses yang ketat dan pengelolaan lalu lintas yang bijaksana menjadi semakin penting. (Raharjo, Bismi, & Purnama, 2023) *Cyber crime* merupakan kejahatan yang dilakukan melalui jaringan internet atau komputer . (Engineering et al., 2023) Dengan perlindungan terhadap ancaman eksternal yang dapat membahayakan jaringan dan mencuri data perusahaan, keamanan jaringan adalah teknik yang digunakan untuk mencegah pencurian data perusahaan.(Prasetyo, Putra, Zulfikri, & Huda, 2023)

Brute force adalah sebuah pendekatan yang langsung (*straight forward*) untuk memecahkan suatu masalah, biasanya didasarkan pada pernyataan masalah (problem statement) dan definisi konsep yang dilibatkan.(Syaputera, Riska, & Mardiana, 2023) serangan *Brute Force* adalah salah satu taktik yang paling umum digunakan oleh peretas untuk mengakses jaringan yang tidak sah. (Bahri, 2023) Dengan dasar ini, menjadi landasan untuk membuat sistem jaringan komputer yang lebih aman, sehingga pada penelitian ini dilakukan Deteksi dan Pencegahan Ekploitasi Jaringan *Brute Force* Menggunakan *Firewall* untuk mengamankan jaringan dari serangan orang-orang yang tidak bertanggung. (Mudzakkar, Siaulhak, & Jumarniati, 2023) *Firewall Filter* bertujuan untuk menyaring packet data yang masuk pada perangkat router. Saat ini, biaya tinggi masih menghalangi pembelian *firewall* yang tangguh. Perangkat *firewall* yang canggih itu hanya dapat diakses oleh instansi besar dan perusahaan kecil. Oleh karena itu, perangkat *firewall* atau keamanan murah diperlukan untuk melindungi jaringan komputer bisnis dan organisasi menengah dan kecil. (Sistim et al., 2024) Sedangkan *Firewall* melakukan filtering terhadap data yang diterima dan melacak koneksi yang dibuat untuk menentukan data apakah koneksi tersebut diizinkan atau ditolak. (Jaya, Yuhandri, & Sumijan, 2020) Dalam pencegahan ini kami menggunakan metode *filtering* melalui *tools addresslist* pada menu *firewall*.

METODE PENELITIAN

Dalam penelitian ini kami membuat kerangka kerja dalam menganalisis dan menemukan solusi pada permasalahan keamanan jaringan.



Sumber : Hasil Penelitian (2024)

Gambar. 1 Kerangka Penelitian

1. Studi Literatur

Studi literatur dilakukan dengan melakukan penelusuran tentang topik penelitian yang akan dilakukan. Jurnal ilmiah, buku, maupun internet yang berkaitan dengan topik penelitian sebelumnya. (Prasetyo et al., 2023)

2. Analisa Masalah

Pada tahapan Analisa ini kami menganalisis kebutuhan pada permasalahan jaringan yang telah kami uji dan kami identifikasi permasalahannya, kemudian kami temukan sebuah solusi menggunakan metode yang tepat. (Raharjo et al., 2023)

3. Rancangan

Pada tahap ini dilakukan pembuatan rancangan skema

yang dibutuhkan mulai dari menyiapkan sisi *hardware* dan juga pada sisi *software*. Menyiapkan tools yang digunakan untuk bisa melakukan simulasi terbaik agar bisa dijalankan dan diterapkan kedalam sistem yang asli.

4. Konfigurasi

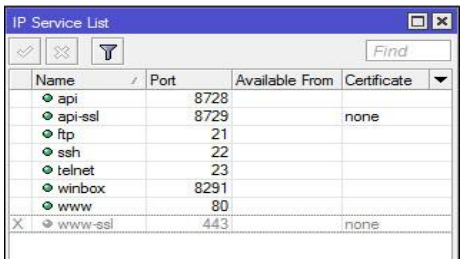
Melakukan konfigurasi pada firewall yang akan menjadi tameng pencegahan terhadap serangan yang terjadi pada jaringan komputer.

5. Pengujian

Tahap pengujian ini dilakukan mulai dari simulasi serangan dan menentukan celah mana saja yang menjadi kelemahan firewall dan setelah diketahui permasalahannya diterapkan dan kemudian di test Kembali agar apa yang telah diterapkan pada rancangan yang telah dikonfigurasi dapat dinyatakan sudah berhasil di uji.

HASIL DAN PEMBAHASAN

Dalam bahasan ini ada satu hal yang menjadi fokus peneliti dalam pembahasan yang merupakan celah kunci terjadi penyerangan terhadap sebuah keamanan jaringan komputer. Protocol TCP/UDP menjadi hal yang bisa menjadi sebuah celah dalam penyerangan jaringan komputer terutama dalam router mikrotik terdapat beberapa pintu masuk untuk mengakses.



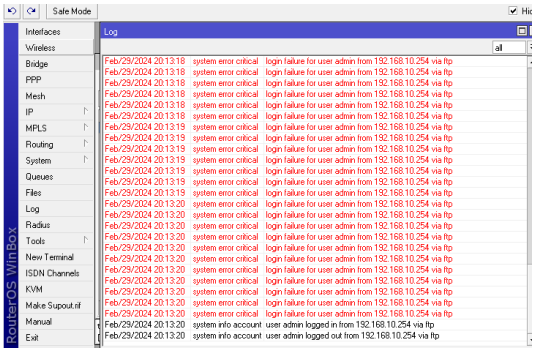
Sumber : Hasil Penelitian (2024)

Gambar. 2 *Service List*

Gambar di atas menjelaskan *port* mana saja yang bisa digunakan dalam mengakses masuk kedalam sistem router mikrotik. Tentu dengan banyaknya pintu masuk akan menjadi celah keamanan yang bisa diretas begitu saja. Namun Solusi yang ditawarkan bukan menutup pintu-pintu tersebut, karna sebagaimana mestinya dipastikan tetap ada satu pintu yang terbuka walaupun sudah digunakan kunci.

1. Analisa Keamanan

Peneliti melakukan tahapan analisis berdasarkan beberapa data yang terjadi terhadap serangan yang terjadi pada *router* melalui *log activity* dan kemudian diputuskan pintu-pintu mana saja yang paling rentan terhadap serangan tersebut.



Sumber : Hasil Penelitian (2024)

Gambar. 3 *Log History Attacking*

Gambar di atas menunjukkan telah terjadinya serangan terhadap router melalui protocol ftp secara *continuous* atau berurutan dengan penyerangan model *brute force* dan berhasil membobol *username* dan *password* dari *router* mikrotik dalam waktu hitungan menit.

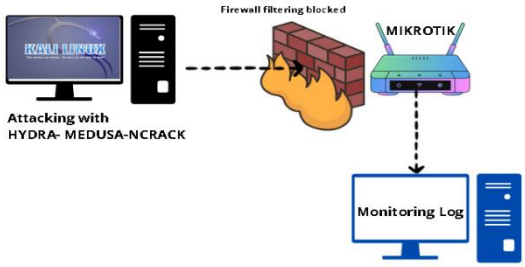
2. Pengujian Serangan

Tabel. 1 Penetration Test

No	Port	Hydra	Medusa	Ncrack
1	*SSH*	Gagal	Berhasil	Gagal
2	*TELNET*	Berhasil	Gagal	Gagal
3	*FTP*	Berhasil	Berhasil	Berhasil
4	*HTTP*	Berhasil	Berhasil	Berhasil
5	*HTTPS*	Gagal	Gagal	Gagal

Sumber : Hasil Penelitian (2024)

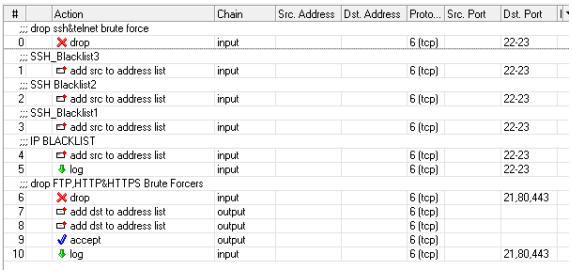
Pada table di atas adalah hasil percobaan penyerangan terhadap router kami yang baru diberikan pengamanan standar berupa *user* dan *password* dan beberapa *tools* yang digunakan pada kali linux seperti hydra,medusa dan *ncrack*. Tingkat keberhasilan pembobolan yang tinggi ditunjukkan pada port *FTP* dan *HTTP* dimana pada tiga *tools* yang digunakan semuanya berhasil membobol *password* tersebut. Pintu masuk tersebut akan diberikan konfigurasi agar serangan-serangan bisa dicegah dengan baik.



Sumber : Hasil Penelitian (2024)

Gambar. 4 Skema Simulasi Serangan dan Pertahanan

Gambar 3 menunjukkan penyerangan dan pertahanan yang dilakukan menggunakan aplikasi simulator virtual box beserta mikrotik os didalamnya dan menginstall kali linux dengan menggunakan tools seperti hydra,medusa dan ncrack.

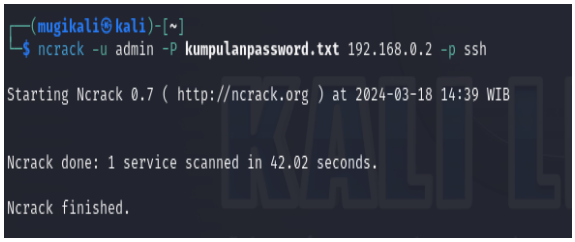


#		Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port
;;; drop ssh&telnet brute force								
0		drop	input			6 (tcp)		22-23
;;; SSH_Blacklist3								
1		add src to address list	input			6 (tcp)		22-23
;;; SSH Blacklist2								
2		add src to address list	input			6 (tcp)		22-23
;;; SSH_Blacklist1								
3		add src to address list	input			6 (tcp)		22-23
;;; IP BLACKLIST								
4		add src to address list	input			6 (tcp)		22-23
5		log	input			6 (tcp)		22-23
;;; drop FTP,HTTP&HTTPS Brute Forcers								
6		drop	input			6 (tcp)		21,80,443
7		add dst to address list	output			6 (tcp)		
8		add dst to address list	output			6 (tcp)		
9		accept	output			6 (tcp)		
10		log	input			6 (tcp)		21,80,443

Sumber : Hasil Penelitian (2024)
Gambar. 5 *Service List*

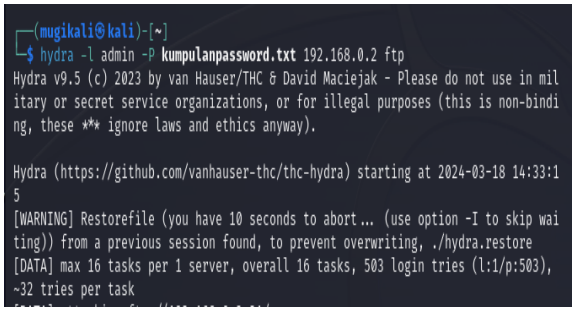
Dalam melakukan konfigurasi, dilakukan pencegahan terhadap serangan *brute force* dari celah *port* seperti *ssh, telnet,ftp, http* dan *https*. Penyaringan terhadap serangan dibagi menjadi 3 (tiga) *level* yaitu *level 1* , *level 2* dan *level 3*. Dengan perbedaan masing-masing yaitu hukuman yang diberikan mulai dari 1 (Satu) hari sampai dengan di *drop* akses selamanya.

Hal ini kemudian dibuktikan dengan percobaan penyerangan yang dilakukan mulai dari menggunakan *ncrack,medusa* dan *hydra* penyerangan dilakukan menuju *router mikrotik* tujuan.



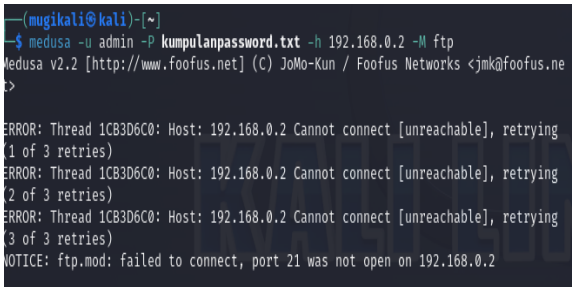
Sumber : Hasil Penelitian (2024)
Gambar. 6 Penyerangan dengan *ncrack*

Penyerangan dengan ncrack terbukti gagal menembus pertahan mikrotik.



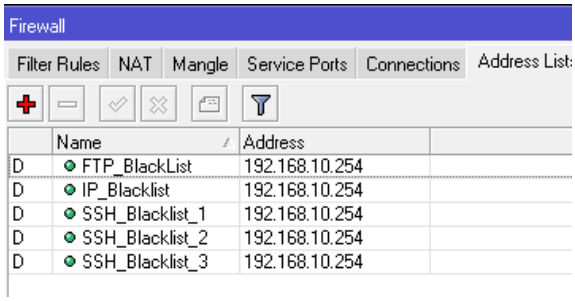
Sumber : Hasil Penelitian (2024)
Gambar. 7 Penyerangan dengan *hydra*

Penyerangan menggunakan hydra juga Kembali gagal menembus pertahanan mikrotik yang telah dijaga dengan *addresslist*.



Sumber : Hasil Penelitian (2024)
Gambar. 8 Penyerangan dengan *medusa*

Penyerangan menggunakan medusa juga Kembali gagal menembus pertahanan mikrotik yang telah dijaga dengan *addresslist*



Sumber : Hasil Penelitian (2024)
Gambar. 9 *Addresslist IP Blacklist*

Pada gambar di atas memperlihatkan ketika terjadi penyerangan *IP* penyerang akan dihukum dengan berbagai *level* tergantung seberapa kali percobaan penyerangan tersebut. Hal ini menunjukkan bahwa pertahanan telah berhasil melakukan pencegahan yang sangat kuat. Sehingga jika ada serangan yang terjadi *IP* penyerang akan langsung terblacklist secara otomatis oleh *firewall* mikrotik.

KESIMPULAN

Dari hasil analisa yang dilakukan terdapat beberapa temuan celah keamanan yang lemah pada router sehingga rentan dimasuki oleh orang lain lewat serangan *brute force* diantaranya adalah *port ssh,telnet,ftp,http dan https*. Kemudian dilakukan pencegahan dengan melakukan konfigurasi pencegahan pada *firewall rules* yang terhubung dengan *addresslist* dimana diberikan 3 (tiga) level penangkapan *IP* penyerang telah diterapkan. Selanjutnya dilakukan ujicoba penyerangan dan pertahanan terhadap sistem yang telah di konfigurasi dan hasilnya menggunakan *tools hacking ncrack,hydra* dan *medusa* tidak ada yang berhasil menembus kedalam pertahanan meskipun sudah

diujicoba berkali-kali, ini mendandakan keberhasilan yang sangat signifikan bagi pertahanan *router.*

REFERENSI

Bahri, S., Info, A., Jaringan, K., Force, S. B., & Mikrotik, R. (2023). Indonesian Journal of Education And Computer Science Perancangan Keamanan Jaringan Untuk Mencegah Terjadinya Serangan Bruteforce Pada Router, *1*(3), 136–147.

Cahya, B., Rizki, F., Sutiyo, A., Saputra, Y. El, & Elfarizi, M. (2023). Implementasi Firewall Pada Mikrotik Untuk Keamanan Jaringan. *Jurnal JOCOTIS-Journal Science Informatica and Robotics E*, *1*(2), 63–80. Diambil dari https://jurnal.ittc.web.id/index.php/jct/

Desmira, & Wiryadinata, R. (2022). Rancang Bangun Keamanan Port Secure Shell (SSH). *Jurnal Inovasi dan Sains Teknik Elektro*, *3*(1), 1–5. Diambil dari http://jurnal.bsi.ac.id/index.php/insantek

Dewi, S., & Islami, A. I. (2021). Implementasi Web Filtering Menggunakan Router Fortigate FG300D. *INSANtek*, *2*(1), 22–27. https://doi.org/10.31294/instk.v2i1.424

Engineering, I., Setiawan, D., Pratama, M. C., Arisandi, D., Informatika, T., & Abdurrab, U. (2023). IMPLEMENTASI SISTEM KEAMANAN JARINGAN MENGGUNAKAN RULE-, *7*(2), 381–389.

Jaya, B., Yuhandri, Y., & Sumijan, S. (2020). Peningkatan Keamanan Router Mikrotik Terhadap Serangan Denial of Service (DoS). *Jurnal Sistim Informasi dan Teknologi*, *2*, 115–123. https://doi.org/10.37034/jsisfotek.v2i4.32

Keamanan Dan Monitoring Jaringan Infrastruktur Di Kantor DPRD Bekasi Faris Jawad, O., Amanda Amalia, R., Sutan Nadzarudien, T., Sistem Informasi, P., & Tinggi Ilmu Komputer Cipta Karya Informatika, S. (2023). Optimizing Security And Monitoring Infrastructure Networks At The Bekasi DPRD Office. *ARSY : Aplikasi Riset kepada Masyarakat*, *184*(2), 184–189.

Mudzakkar, Siaulhak, & Jumarniati. (2023). Brute Force Exploit Menggunakan Firewall Pada Kantor Bappeda Kota Palopo. *Sibatik Journal | Volume*, *2*(4), 1097–1106. Diambil dari https://publish.ojs-indonesia.com/index.php/SIBATIK

Prasetyo, F., Putra, E., Zulfikri, A., & Huda, M. A. (2023). Analisis Keamanan Jaringan Dari Serangan Malware Menggunakan Firewall Filtering Dengan Port Blocking, *3*(2), 857–863.

Raharjo, M., Bismi, W., & Purnama, R. A. (2023). Optimizing Network Security Point to Point with ACL Filtering and TTL Methods, *5*(2).

Shafiyyah, A., Elektro, J. T., Teknik, F., & Lampung, U. (2024). Implementasi sistem keamanan jaringan di psdku universitas lampung waykanan menggunakan server wazuh untuk deteksi dan respon serangan siber.

Sistim, J., Prasetyo, F., Putra, E., Hamzah, A., Agel, W., & Kusuma, R. O. F. (2024). Impelementasi Sistem Keamanan Jaringan Mikrotik Menggunakan Firewall Filtering dan Port Knocking, *5*(4), 82–87. https://doi.org/10.60083/jsisfotek.v5i4.329

Syaputera, A., Riska, R., & Mardiana, Y. (2023). Hotspot Network Security System From Brute Force Attack Using Pfsense External Firewall (Case Study of Wifi-Ku.Net Hotspot). *Jurnal Komputer, Informasi dan Teknologi (JKOMITEK)*, *3*(1), 205–218. https://doi.org/10.53697/jkomitek.v3i1.1286

Watmah, S. (2022). Implementasi Queue tree Pada Jaringan Komputer BPRS Bumi Artha. *INSANtek*, *3*(1), 18–22. https://doi.org/10.31294/instk.v3i1.1163

Yudi mulyanto, M. Julkarnain, & Jabi Afahar, A. (2021). Implementasi Port Knocking Untuk Keamanan Jaringan Smkn 1 Sumbawa Besar. *Jurnal Informatika Teknologi dan Sains*, *3*(2), 326–335. https://doi.org/10.51401/jinteks.v3i2.1016