Jurnal Review Pendidikan dan Pengajaran
http://journal.universitaspahlawan.ac.id/index.php/jrpp
Volume 8 Nomor 1, 2025
P-2655-710X e-ISSN 2655-6022

Submitted : 29/01/2025
Reviewed : 02/02/2025
Accepted : 02/02/2025
Published : 05/02/2025

Fachroni Arbi Murad [1]
Asep Kurniawan[2]
Muhammad Yusuf Bagus Rasyiidin[3]

PORT KNOCKING PADA MIKROTIK UNTUK MENINGKATKAN KEAMANAN WIFI DI ERA INDUSTRI 4.0

Abstrak
Keamanan jaringan menjadi salah satu elemen utama yang harus diperhatikan dalam era Industri 4.0, di mana peran konektivitas WiFi sangat penting untuk mendukung proses otomatisasi dan komunikasi. Studi ini berfokus pada analisis dan implementasi mekanisme keamanan Multiple Port Knocking pada perangkat Mikrotik untuk meningkatkan perlindungan akses WiFi. Teknik Port Knocking bekerja dengan cara mengautentikasi pengguna melalui serangkaian pola koneksi ke port tertentu sebelum akses diizinkan, sehingga mampu mencegah akses ilegal. Dalam penelitian ini, digunakan pendekatan NDLC (Network Development Life Cycle) untuk merancang, mengimplementasikan, dan mengevaluasi Multiple Port Knocking pada jaringan WiFi. Hasil pengujian menunjukkan bahwa metode ini mampu mengurangi risiko serangan seperti brute force dan akses tidak sah, sekaligus memungkinkan integrasi dengan sistem keamanan lain tanpa menurunkan performa jaringan secara signifikan. Dengan kemudahan implementasi dan fleksibilitas yang tinggi, Multiple Port Knocking menjadi solusi efektif dan efisien untuk meningkatkan keamanan jaringan WiFi berbasis Mikrotik di tengah perkembangan era digital.
Kata Kunci: Multiple Port Knocking, Mikrotik, Keamanan WiFi, Era Industri 4.0, NDLC

Abstract
Network security is one of the main elements that must be considered in the Industry 4.0 era, where the role of WiFi connectivity is very important to support automation and communication processes. This study focuses on the analysis and implementation of Multiple Port Knocking security mechanisms on Mikrotik devices to increase WiFi access protection. The Port Knocking technique works by authenticating users through a series of connection patterns to certain ports before access is permitted, thereby preventing illegal access. In this research, the NDLC (Network Development Life Cycle) approach is used to design, implement and implement Multiple Port Knocking on WiFi networks. Test results show that this method is able to reduce the risk of attacks such as brute force and unauthorized access, while allowing integration with other security systems without significantly reducing network performance. With high ease and instant implementation, Multiple Port Knocking is an effective and efficient solution for increasing the security of Mikrotik-based WiFi networks amidst the development of the digital era.
Keywords: Multiple Port Knocking, Mikrotik, WiFi Security, Industrial Era 4.0, NDLC

PENDAHULUAN

Dengan pesatnya perkembangan teknologi di Era Industri 4.0, kebutuhan terhadap jaringan yang andal dan sesuai kebutuhan terus meningkat. Dan banyak perusahaan yang telah memanfaatkan kemajuan teknologi komputer, terutama dengan menggunakan Teknologi Jaringan Komputer, baik melalui jaringan intranet maupun internet.[1]Teknologi terus berkembang, didukung dengan sarana dan prasarana yang memadai, sangat membutuhkan jaringan yang mampu beroperasi dengan baik.[2] Jaringan memiliki peran penting, terutama dalam aktivitas yang membutuhkan kestabilan koneksi, seperti di perguruan tinggi, perkantoran, industri, bisnis. Aktivitas di perguruan tinggi, perkantoran, dan industry, bisnis membutuhkan jaringan yang mendukung transfer data optimal, Menjadi kunci kelancaran pengiriman data untuk membentuk jaringan yang baik, diperlukan perangkat keras atau perangkat lunak yang

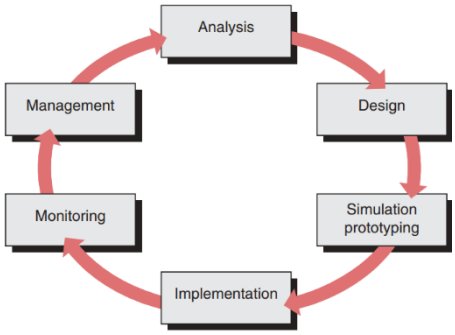
[1,2,3] Jurusan Teknik Informatika dan Komputer, Politeknik Negeri Jakarta, Depok
email:fachroni.murad@tik.pnj.ac.id, Asep.kurniawan@tik.pnj.ac.id, muhammad.yusufbr@gmail.com

mendukung, salah satu perangkat tersebut adalah Mikrotik. Mikrotik merupakan sistem operasi yang dilengkapi dengan perangkat lunak untuk mengelola jaringan router.[3] Dalam pengelolaan router Mikrotik, keamanan akses ke router menjadi aspek penting yang harus diperhatikan, agar konfigurasi tetap terlindungi dan router aman dari ancaman pihak yang tidak bertanggung jawab untuk melindungi router, diperlukan konfigurasi yang tepat. Salah satu metode yang dapat digunakan untuk mengamankan router adalah port knocking. Port Knocking adalah teknik yang digunakan untuk membuka akses port tertentu yang sebelumnya diblokir oleh Firewall[4], dengan mengirimkan koneksi atau data dalam pola tertentu sebagai kunci akses.[5]Port knocking adalah sistem keamanan yang membuka port terblokir dengan memberikan aturan tertentu melalui siapa yang benar-benar berhak masuk kedalam router.[6] Oleh karena itu port yang akan di lindungi adalah port 21 (ftp), port 22 (SSH) dan port 8291 (Winbox). [7] Masalah umum yang sering terjadi dalam penyediaan layanan internet, seperti pada keamanan jaringan Mikrotik, adalah terkait dengan pengelolaan hak akses. Hal ini disebabkan adanya kemungkinan pengguna tidak diinginkan yang mencoba mengakses koneksi jaringan Mikrotik, sehingga dapat mengancam keamanan jaringan tersebut.[8], [9]

Dalam penelitian ini, metode port knocking[10] dikembangkan dengan menambahkan fitur seperti Port Sequence Trigger, sehingga tingkat keamanan pada router Mikrotik menjadi lebih baik dan lebih sulit untuk ditembus. penelitian ini dapat meningkatkan pemahaman tentang konfigurasi dan implementasi keamanan pada router Mikrotik.

METODE

Pendekatan atau tahapan yang diterapkan dalam penelitian ini menggunakan metode NDLC (Network Design Life Cycle),[11], [12], [13], [14], [15] sehingga seluruh rangkaian proses penelitian dapat dilaksanakan dengan terstruktur, sistematis, dan terarah sesuai gambar 1.



Gambar 1 Tahapan metode penelitian

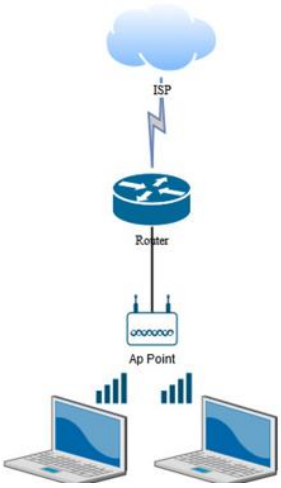
Penelitian ini menggunakan metode NDLC (Network Development Life Cycle), dengan pendekatan beberapa tahapan yang meliputi:

1. Analisis, Tahap ini bertujuan untuk menganalisis kebutuhan sistem, permasalahan yang dihadapi, harapan pengguna, dan pemilihan topologi jaringan yang paling sesuai. Data yang diperoleh dijadikan dasar untuk merumuskan masalah utama yang harus dipecahkan, khususnya terkait keamanan jaringan. Proses analisis juga melibatkan identifikasi sistem jaringan yang sedang digunakan, sehingga dapat memberikan gambaran awal mengenai pengembangan sistem yang akan diterapkan di masa depan. Hasil identifikasi ini mempermudah perencanaan sistem yang sesuai dengan kebutuhan.
2. Desain, Pada tahap desain, dilakukan perancangan topologi jaringan keamanan berdasarkan kondisi jaringan saat ini. Penelitian ini menggunakan perangkat Mikrotik, dengan pendekatan topologi jaringan berbentuk tree. Proses desain melibatkan pembuatan diagram dan rancangan teknis yang akan menjadi acuan untuk implementasi berikutnya. Langkah ini bertujuan memastikan sistem dirancang secara efektif untuk memenuhi standar keamanan yang dibutuhkan.
3. Simulasi, Setelah desain selesai, dilakukan simulasi untuk memvisualisasikan cara kerja sistem yang telah dirancang. Simulasi ini dilakukan dengan membangun infrastruktur jaringan menggunakan perangkat Mikrotik. Tujuan simulasi adalah untuk menguji performa awal sistem serta menilai sejauh mana sistem yang dirancang dapat memenuhi kebutuhan dan menghadapi skenario penggunaan yang telah diprediksi.

4. Implementasi, Tahap implementasi melibatkan penerapan sistem yang telah dirancang ke dalam jaringan yang sedang berjalan. Proses ini membutuhkan waktu yang relatif lama karena mencakup instalasi, konfigurasi, dan integrasi dengan sistem yang ada. Melalui tahap ini, akan terlihat bagaimana sistem yang baru berfungsi dalam lingkungan nyata, serta potensi perbaikan yang diperlukan untuk menyempurnakan kinerjanya.
5. Monitoring, Setelah sistem diterapkan, dilakukan pemantauan secara berkala untuk mengevaluasi performa dan stabilitasnya. Tahap ini penting untuk memastikan sistem mampu menghadapi berbagai ancaman keamanan. Administrator jaringan bertugas mengawasi lalu lintas data, memeriksa kelancaran sistem, dan memastikan semua transaksi data berjalan dengan aman. Pemantauan ini juga bertujuan mendeteksi potensi kelemahan yang mungkin muncul.
6. Manajemen, Pada tahap akhir, dilakukan pengelolaan dan pemeliharaan sistem untuk menjamin keberlangsungan operasionalnya. Sistem yang telah diterapkan perlu dirawat dengan baik agar tetap stabil dan mampu berfungsi dalam jangka panjang. Jika ditemukan kerentanan atau masalah keamanan, perbaikan dilakukan secara optimal, dan jika diperlukan, implementasi ulang dapat dilakukan. Tahap ini memastikan sistem tetap relevan dan aman dari potensi ancaman di masa mendatang.

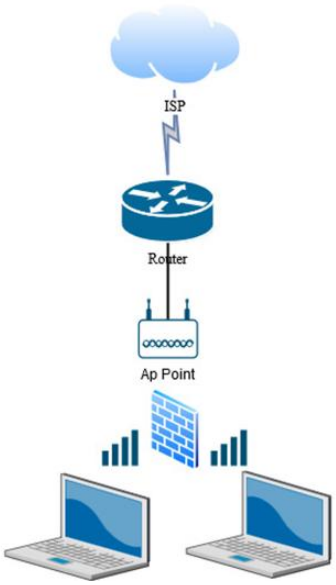
HASIL DAN PEMBAHASAN

Berdasarkan hasil analisis dan pengujian yang telah dilakukan, ditemukan bahwa konfigurasi port knocking pada router Mikrotik mampu bekerja dengan optimal, memberikan perlindungan yang efektif terhadap ancaman jaringan. Router Mikrotik sendiri berperan sebagai objek utama dalam penelitian ini, di mana metode port knocking diterapkan sebagai langkah keamanan untuk mencegah serangan seperti spoofing attack, brute force attack, dan port scanning. Sebagai fitur bawaan Mikrotik, port knocking dirancang untuk meningkatkan keamanan akses port dengan cara mengontrol akses hanya setelah pola knock tertentu diterapkan sesuai dengan aturan (rule) yang telah ditetapkan. Metode ini memastikan keamanan jaringan tetap terjaga dengan memberikan kontrol ketat terhadap akses port yang sebelumnya diblokir.



Gambar 2 Topologi Jaringan

Pada gambar 2 adalah Data dikomunikasikan antara user dan router melalui perangkat jaringan, seperti router Mikrotik, dan access point. Router Mikrotik, memberikan ip dynamic host control protocol (DHCP) ke user melalui access point.

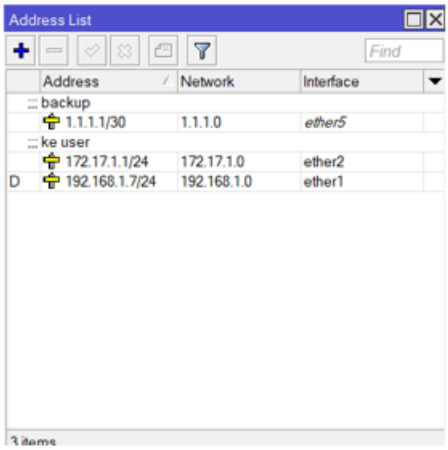


Gambar 3 Port Knocking

Gambar 3 menjelaskan topologi proses port knocking menggunakan aturan firewall bekerja dengan memblokir secara otomatis semua aturan yang belum diaktifkan oleh router. Pendekatan ini sangat efektif dalam meningkatkan keamanan, mengingat komunikasi melalui port sering kali menjadi target eksploitasi oleh pihak yang tidak bertanggung jawab.

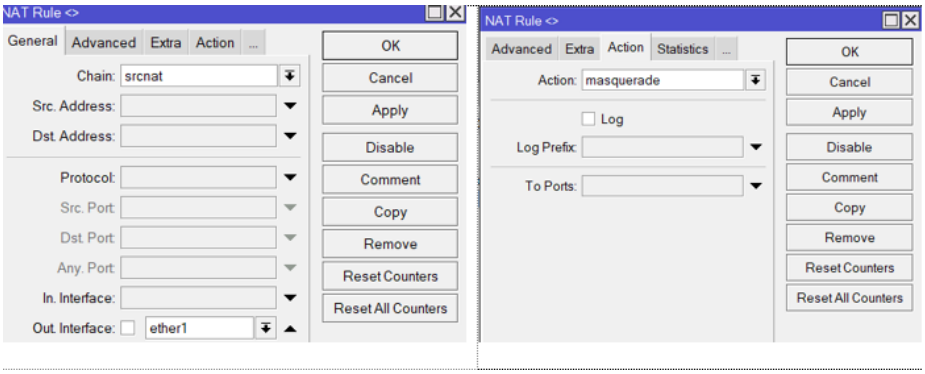
Instalasi dan Konfigurasi

Tahapan pertama yang harus dilakukan adalah melakukan pengaturan ethernet 2 karena ethernet 2 yang terhubung ke access point dan media komunikasi yang pertama digunakan oleh pengguna dilokasi, seperti gambar 4 :



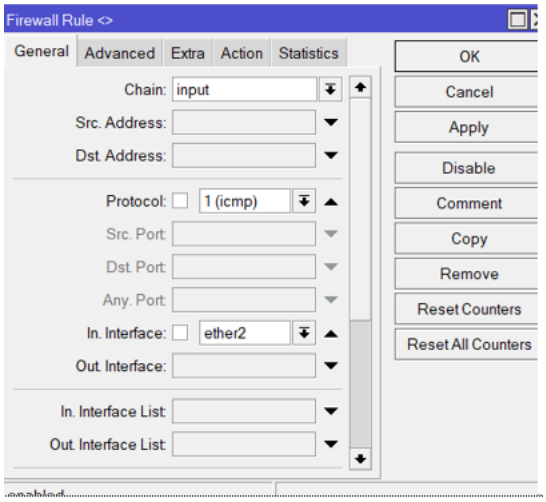
Gambar 4 koneksi pada ethernet 2

Konfigurasi NAT (Network Address Translation) pada gambar 5 menunjukkan pengaturan untuk menerjemahkan alamat IP perangkat di jaringan lokal agar dapat mengakses internet. Pengaturan seperti chain, alamat sumber dan tujuan, protokol, port, dan antarmuka masuk dan keluar menentukan bagaimana proses penerjemahan alamat IP ini dilakukan. Dengan konfigurasi NAT yang benar, perangkat di jaringan lokal dapat terhubung ke internet.



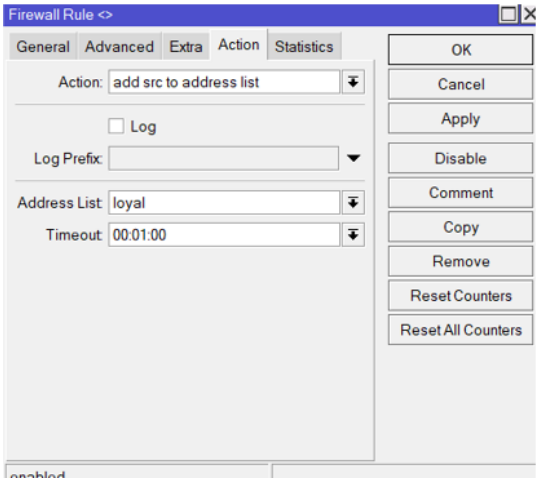
Gambar 5 Proses Nat

Konfigurasi firewall rule pada gambar 6 menunjukkan pengaturan untuk memeriksa dan mengontrol lalu lintas jaringan yang masuk ke perangkat MikroTik melalui antarmuka ether2. Aturan ini secara khusus dirancang untuk memeriksa paket ICMP (Internet Control Message Protocol), yang sering digunakan untuk mengirim pesan kesalahan dan informasi.



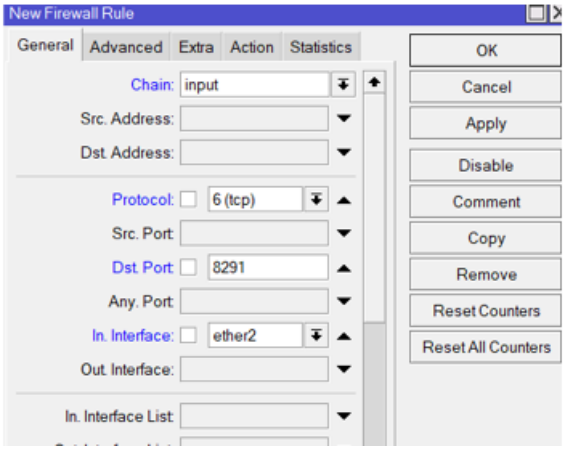
Gambar 6 Port Knocking

Membuat konfigurasi sebuah aturan firewall yang memiliki tindakan khusus, yaitu add src to address list. ketika ada paket data yang sesuai dengan aturan ini, alamat IP sumber dari paket tersebut akan ditambahkan ke dalam sebuah daftar alamat yang bernama "loyal". Daftar alamat ini bisa digunakan untuk berbagi tujuan, untuk membuat aturan firewall lainnya yang lebih spesifik berdasarkan daftar alamat tersebut, atau untuk memonitor aktivitas jaringan. Selain itu, terdapat opsi "Log" yang jika dicentang akan mencatat setiap kali aturan ini aktif. Opsi "Timeout" menentukan berapa lama alamat IP akan tetap berada dalam daftar sebelum dihapus secara otomatis pada gambar 7.



Gambar 7 Timeout

Konfigurasi firewall rule menunjukkan pengaturan untuk memeriksa dan mengontrol lalu lintas jaringan yang masuk ke perangkat mikrotik melalui antarmuka ether2. Aturan ini secara khusus dirancang untuk memeriksa paket TCP (Transmission Control Protocol)menggunakan port tujuan 8291 pada gambar 8.



Gambar 8 port 8291

Pesan Connecting to 172.17.1.1 mengindikasikan bahwa perangkat saat ini sedang mencoba untuk terhubung ke perangkat jaringan. Proses ini tidak terkoneksi ini sebelum menggunakan knocking pada port yang sudah di buat dengan mencoba masuk ke winbox tanpa knocking pada gambar

Gambar 9 tidak bisa masuk ke winbox

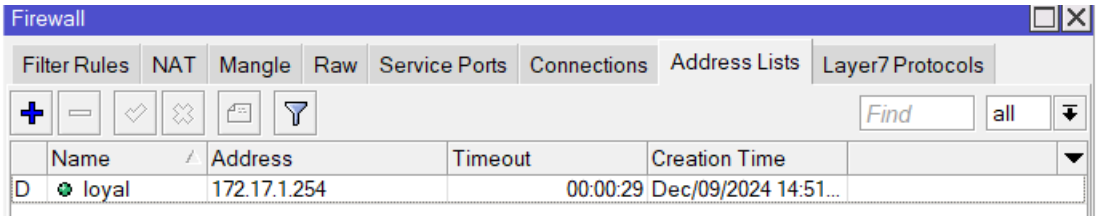
Output di ini menunjukkan hasil dari perintah ping 172.17.1.1 dijalankan pada sebuah perangkat. Perintah ping digunakan untuk menguji keterhubungan dan proses knocking ke perangkat jaringan dengan mengirimkan paket data.

```
C:\Users\Roni>ping 172.17.1.1

Pinging 172.17.1.1 with 32 bytes of data:
Reply from 172.17.1.1: bytes=32 time<1ms TTL=64
Reply from 172.17.1.1: bytes=32 time=1ms TTL=64
Reply from 172.17.1.1: bytes=32 time<1ms TTL=64
Reply from 172.17.1.1: bytes=32 time=1ms TTL=64
```

Gambar 10 pross ping

Tampilan antarmuka sebuah perangkat jaringan menampilkan daftar alamat IP yang telah berhasil masuk ke dalam router. Daftar ini berada di bawah tab Address Lists pada gambar 11.



Gambar 11 address list

Sebelum melakukan seranga seorang hacker mengumpulkan data dari paket-paket yang melintas di jaringan. Dalam data tersebut terdapat data penting berupa clear teks atau password hal ini perlu dilakukan untuk mengukur seberapa aman jaringan yang ada berikut table 1 di bawah ini.

Tabel 1 Scanning port

No	Port	Service	Status
1	21	FTP	Open
2	23	Telnet	Open
3	22	SSH	Open
4	8291	Winbox	Open

Tabel 2 Memperlihatkan hasil pengujian serangan port scanning dan mendapatkan informasi berupa port yang terbuka.

SIMPULAN

Penelitian ini membuktikan bahwa implementasi Port Knocking pada perangkat Mikrotik efektif dalam meningkatkan keamanan jaringan WiFi di era Industri 4.0. Metode ini memberikan lapisan perlindungan tambahan dengan hanya memberikan akses kepada pengguna yang telah memenuhi pola autentikasi tertentu, sehingga dapat mencegah serangan seperti brute force dan akses tidak sah. Selain itu, Port Knocking dapat diintegrasikan dengan mudah ke dalam infrastruktur jaringan yang sudah ada tanpa mengganggu performa secara signifikan. Dengan fleksibilitas dan efisiensinya, pendekatan ini menjadi solusi yang relevan untuk mengatasi tantangan keamanan dalam konektivitas WiFi di tengah perkembangan teknologi yang pesat

SARAN

Untuk pengembangan lebih lanjut, direkomendasikan agar metode Port Knocking diintegrasikan dengan mekanisme keamanan lain, seperti VPN atau firewall berbasis kecerdasan buatan, untuk mengatasi ancaman yang lebih kompleks. Selain itu, pengujian pada jaringan dengan skala yang lebih besar perlu dilakukan guna menilai efektivitas metode ini dalam berbagai situasi. Edukasi kepada pengguna mengenai pentingnya menjaga kerahasiaan pola akses juga menjadi langkah penting untuk mendukung keberhasilan implementasi Port Knocking. Pengembangan alat bantu untuk otomatisasi konfigurasi direkomendasikan agar proses pengaturan dan pemeliharaan sistem menjadi lebih sederhana, terutama bagi administrator jaringan dengan tingkat keahlian yang beragam. Pemantauan dan evaluasi secara

berkelanjutan sangat diperlukan agar metode ini tetap relevan dan mampu menghadapi tantangan keamanan yang terus berkembang di era digital.

DAFTAR PUSTAKA

A. Widodo, 'IMPLEMENTASI MONITORING JARINGAN KOMPUTER MENGGUNAKAN DUDE'.

H. Amalia, T. Retnasari, and S. Rachmawati, 'Pemanfaatan Teknologi Informasi Untuk Meningkatkan Pelayanan Akademik Rumah Tahfidz dan TPQ Sakinah Cipayung Jakarta Timur', 2020. [Online]. Available: http://ejournal.bsi.ac.id/ejurnal/index.php/abdimas

A. Zainy et al., 'INSTALASI MIKROTIK PADA VIRTUALBOX DAN PENGKONEKSIAN ANTARA MIKROTIKDI VIRTUALBOX DENGAN WINBOX DI SMK S TERUNA PADANG SIDEMPUAN of Knowing How to Install Mikrotik on VirtualBox and Connecting Mikrotik to Winbox at SMKS Teruna Padangsidimpuan', 2023. [Online]. Available: https://jurnal.spada.ipts.ac.id/index.php/adam

B. Cahya, F. Rizki, A. Sutiyo, Y. El Saputra, and M. Elfarizi, 'IMPLEMENTASI FIREWALL PADA MIKROTIK UNTUK KEAMANAN JARINGAN', 2023. [Online]. Available: https://jurnal.ittc.web.id/index.php/jct/

A. Saputro, N. Saputro, and H. Wijayanto, 'METODE DEMILITARIZED ZONE DAN PORT KNOCKING UNTUK KEAMANAN JARINGAN KOMPUTER', 2020.

M. Idhom, H. E. Wahanani, and A. Fauzi, 'Network Security Applications Using the Port Knocking Method', in Journal of Physics: Conference Series, IOP Publishing Ltd, Jul. 2020. doi: 10.1088/1742-6596/1569/2/022046.

J. Pendidikan and D. Konseling, 'Analisis Keamanan Website Universitas Singaperbangsa Karawang Menggunakan Metode Vulnerability Assessment'.

S. Esabella and Y. Bella Fitriana, 'KLIK: Kajian Ilmiah Informatika dan Komputer Analisis Keamanan Jaringan Menggunakan Metode Security Policy Development Life Cycle (SPDLC)', Media Online, vol. 4, no. 1, pp. 634–641, 2023, doi: 10.30865/klik.v4i1.1157.

M. Muhallim and S. Paembonan, 'Rancang Bangun Sistem Keamanan Jaringan Menggunakan Metode Port Knocking Dan Port Blocking Dengan Notifikasi Email Pada SMK Kartika XX-2 Palopo'. [Online]. Available: https://ojs.unanda.ac.id/index.php/jutinda

N. A. Santoso, K. B. Affandi, and R. D. Kurniawan, 'Implementasi Keamanan Jaringan Menggunakan Port Knocking', Jurnal Janitra Informatika dan Sistem Informasi, vol. 2, no. 2, pp. 90–95, Oct. 2022, doi: 10.25008/janitra.v2i2.156.

Haeruddin and Efendi, '"Rancangan Dan Konfıgurası Jarıngan Pada PT. Samudera Idola Rahayu"', 2021. [Online]. Available: https://journal.uib.ac.id/index.php/conescintech

M. J. Komputer et al., 'Computer Network Management Using a Mikrotik Router at the Immigration Office Class I TPI Bengkulu City', 2022.

Rahmi Ningsy Guncya, D. Dasril, and M. Muhallim, 'Rancang Bangun Sistem Autentikasi Hotspot Berbasis Radius Server Menggunakan Mikrotik Pada Sekolah Menengah Kejuruan Negeri 5 Luwu', Mars : Jurnal Teknik Mesin, Industri, Elektro Dan Ilmu Komputer, vol. 2, no. 3, pp. 138–152, Jun. 2024, doi: 10.61132/mars.v2i3.150.

J. Jamaluddin, Muhammad Zamroni Uska, R. H. Wirasasmita, and M. Roziki, 'Development of Smart Servers for Informatics Education Program Using NDLC Method', JOURNAL OF INFORMATICS AND TELECOMMUNICATION ENGINEERING, vol. 7, no. 2, pp. 597–606, Jan. 2024, doi: 10.31289/jite.v7i2.10853.

H. Wijayanto Aripradono, 'Prosiding National Conference for Community Service Project (NaCosPro)', [Online]. Available: http://journal.uib.ac.id/index.php/nacospro