JUNIF: Jurnal Nasional Informatika

p-ISSN: 2774-3497
e-ISSN: 2774-3500

Vol. 6 No. 1, 15 April 2025, pp. 1-6

IMPLEMENTASI KEAMANAN JARINGAN MIKROTIK MENGGUNAKAN TEKNIK PORT KNOCKING PADA TAMAN MARGASATWA RAGUNAN

PENULIS

[1)]Muhammad Rezky Akbar Sembiring

ABSTRAK

Penelitian ini membahas implementasi port knocking pada perangkat Mikrotik RouterOS sebagai mekanisme penguatan keamanan jaringan. Port knocking digunakan untuk menyembunyikan port layanan penting dengan cara memberikan akses hanya setelah urutan port tertentu berhasil dipanggil oleh pengguna yang sah. Metode ini terbukti mampu menurunkan potensi akses ilegal dan meminimalkan percobaan intrusi yang umum terjadi pada jaringan publik maupun semi publik. Hasil pengujian menunjukkan bahwa konfigurasi port knocking dapat berjalan stabil tanpa memberikan dampak signifikan terhadap performa jaringan. Latensi, throughput, dan ketersediaan layanan tetap berada pada batas toleransi operasional, sehingga metode ini layak diterapkan dalam lingkungan nyata. Pada studi kasus Taman Margasatwa Ragunan, sistem mampu meningkatkan tingkat keamanan akses perangkat jaringan sekaligus mempertahankan kemudahan penggunaan oleh administrator. Berdasarkan temuan tersebut, port knocking dinilai efektif dan efisien sebagai lapisan keamanan tambahan untuk mencegah serangan tidak sah pada infrastruktur jaringan di area semi publik seperti Taman Margasatwa Ragunan. Metode ini dapat diterapkan dengan tingkat kompleksitas yang rendah serta memberikan manfaat signifikan dalam menjaga integritas jaringan.

Kata Kunci

Port Knocking; Mikrotik RouterOS; Keamanan Jaringan; Firewall; Intrusion Prevention; Akses Ilegal; Semi Publik;

AFILIASI

Prodi, Fakultas — [1)] Program Studi Sistem Informasi, Fakultas Ilmu Komputer.
Nama Institusi — [1)] Institut Bisnis dan Informatika Kosgoro 1957.
Alamat Institusi — [1)] Jl. Moh Kahfi II, Srengseng Sawah, Jagakarsa, Jakarta Selatan, DKI Jakarta.

KORESPONDENSI

Penulis — Muhammad Rezky Akbar Sembiring
Email — mrezkyakbarsembiring27@gmail.com

DOI : https://doi.org/10.55122/junif.v6i1.1945

I. PENDAHULUAN

Perkembangan teknologi informasi yang semakin pesat telah menjadikan jaringan komputer sebagai komponen vital dalam operasional berbagai instansi, termasuk fasilitas layanan publik seperti Taman Margasatwa Ragunan. Infrastruktur jaringan digunakan untuk mendukung proses administrasi, layanan tiket elektronik, sistem pengawasan, hingga komunikasi internal antarunit. Ketergantungan yang tinggi terhadap jaringan membawa konsekuensi berupa meningkatnya risiko keamanan, terutama ancaman akses tidak sah yang dapat mengganggu keberlangsungan layanan. Meningkatnya ancaman keamanan tidak selalu harus diatasi dengan membangun sistem jaringan yang sangat mahal dan kompleks. Sebaliknya, diperlukan solusi yang efektif, efisien, dan tetap mempertimbangkan keterbatasan biaya operasional. Salah satu pendekatan yang relevan untuk kebutuhan tersebut adalah penggunaan teknik port knocking. Port knocking merupakan mekanisme autentikasi tersembunyi yang bekerja dengan menutup seluruh port tertentu dan hanya membukanya ketika urutan permintaan port yang benar dikirimkan oleh pengguna yang berwenang. Port knocking diterapkan pada perangkat Mikrotik RouterOS sebagai upaya untuk meningkatkan keamanan jaringan tanpa menurunkan performa operasional. Implementasi dilakukan pada lingkungan semi publik di Taman Margasatwa Ragunan untuk mengevaluasi kemampuan teknik ini dalam mencegah akses tidak sah serta menilai efektivitasnya dalam konteks jaringan yang digunakan secara luas oleh berbagai pihak.

Integrasi Firewall Filtering dengan notifikasi real-time menerapkan konsep defense in depth, di mana firewall tidak hanya memblokir atau mengizinkan lalu lintas jaringan, tetapi juga mendeteksi dan melaporkan ancaman secara otomatis kepada administrator. Firewall Mikrotik melakukan stateful inspection untuk memeriksa status koneksi dan dipadukan dengan Port Knocking sehingga layanan penting tetap tersembunyi hingga proses autentikasi berhasil. Setiap aktivitas mencurigakan, seperti brute force atau port scanning, dicatat dan langsung dikirim melalui bot Telegram menggunakan API, sehingga administrator dapat merespons ancaman dalam hitungan detik. Selain itu, firewall menerapkan manajemen akses dinamis dengan memasukkan alamat IP yang berhasil melakukan Port Knocking ke dalam address list untuk waktu tertentu. Pendekatan ini meningkatkan keamanan jaringan melalui penyembunyian layanan, deteksi dini, dan respons cepat, sehingga memperkecil peluang keberhasilan serangan, terutama yang dilakukan secara otomatis [1]. Network Development Life Cycle (NDLC) yang dibahas dalam jurnal ini merupakan kerangka kerja metodologis yang krusial dalam perancangan dan peningkatan infrastruktur jaringan. Berbeda dengan pendekatan ad-hoc di mana keamanan diterapkan secara acak, NDLC menawarkan siklus berkelanjutan yang terdiri dari tahapan Analysis, Design, Simulation/Prototyping, Implementation, Monitoring, dan Management. Dalam konteks keamanan jaringan Mikrotik, teori ini menegaskan bahwa implementasi teknologi seperti Port Knocking tidak boleh dilakukan secara isolasi, melainkan harus didasarkan pada analisis kebutuhan yang mendalam dan pemahaman terhadap masalah yang ada (seperti manajemen bandwidth yang buruk atau adanya penyusup) [2].

Transport dan Internet pada model referensi TCP/IP untuk menjelaskan bagaimana Port Knocking memanipulasi protokol standar untuk tujuan autentikasi. Secara teoretis, Port Knocking adalah metode komunikasi di mana informasi dikodekan ke dalam urutan paket yang ditujukan ke port tertutup. Teori ini menjelaskan bahwa router Mikrotik tidak membuka port secara permanen. Sebaliknya, router mendengarkan (listening) pola kedatangan paket TCP (misalnya, paket SYN) pada urutan port tertentu (contoh: port 1000, lalu 2000, lalu 3000). Hanya jika urutan ini terpenuhi secara presisi, router memodifikasi aturan firewall internalnya [3].

Inti dari teori ini adalah pemanfaatan flags pada header TCP. Paket yang dikirimkan untuk "mengetuk" port sebenarnya tidak perlu membentuk koneksi penuh (full handshake). Teori ini menjelaskan bahwa firewall dapat dikonfigurasi untuk mendeteksi upaya koneksi awal (SYN packet) ke port tertentu dan mencatat alamat IP pengirim ke dalam daftar alamat sementara (address list) dengan waktu hidup (Time To Live - TTL) yang sangat pendek. Mekanisme ini menciptakan lapisan autentikasi yang tidak terlihat (stealth authentication),

karena bagi pengamat eksternal atau penyerang, port tersebut terlihat tertutup (closed) atau terfilter (filtered), dan tidak ada layanan yang merespons.

Berfokus pada anatomi serangan Brute Force dan bagaimana arsitektur keamanan jaringan harus dirancang untuk memitigasinya. Brute Force didefinisikan sebagai metode serangan coba-coba (trial and error) di mana penyerang menggunakan perangkat lunak otomatis untuk menebak kombinasi username dan password guna mendapatkan akses tidak sah. Teori ini menjelaskan bahwa kelemahan utama yang dieksploitasi oleh Brute Force adalah ketersediaan halaman login atau antarmuka autentikasi yang terbuka untuk umum. Selama port layanan (seperti SSH port 22 atau Winbox port 8291) terbuka, penyerang memiliki kesempatan tak terbatas untuk mencoba membobolnya [4]. Berbeda dengan aksi firewall standar seperti Drop (membuang paket diam-diam) atau Reject (menolak paket dengan pesan error), Tarpit bekerja dengan cara menerima koneksi TCP yang masuk tetapi tidak pernah memproses data di dalamnya. Secara teoretis, Tarpit menjebak penyerang dalam koneksi "zombie". Ketika penyerang (atau alat scanning otomatis) mencoba menghubungkan diri ke port yang dilindungi Tarpit, router seolah-olah membuka koneksi (zero window size), memaksa mesin penyerang untuk menunggu respons yang tidak akan pernah datang, sehingga menghabiskan sumber daya di sisi penyerang dan memperlambat proses pemindaian mereka secara signifikan [5].

Penelitian ini memperluas cakupan keamanan jaringan dari sekadar pencegahan intrusi menjadi ketahanan sistem secara keseluruhan (system resilience). Setyowibowo dkk. berargumen bahwa tidak ada sistem keamanan yang 100% kebal. Oleh karena itu, teori keamanan holistik harus mencakup mekanisme pemulihan (recovery) yang cepat jika terjadi kegagalan sistem, baik akibat serangan siber yang berhasil, kesalahan konfigurasi manusia (human error), atau kegagalan perangkat keras. Fitur Automated Backup pada Mikrotik menjadi komponen teoretis kunci untuk menjamin ketersediaan layanan (Availability) yang berkelanjutan [6]. Teori ini menghubungkan Port Knocking sebagai langkah preventif dengan Automated Backup sebagai langkah kuratif. Dalam skenario di mana seorang penyerang mungkin berhasil melewati lapisan keamanan atau melakukan serangan perusakan (destructive attack) yang menghapus konfigurasi router, administrator harus memiliki kemampuan untuk mengembalikan kondisi sistem ke titik terakhir yang diketahui baik (last known good configuration). Mekanisme pencadangan otomatis yang dikirimkan via email (menggunakan skrip SMTP dan Scheduler Mikrotik) memastikan bahwa salinan konfigurasi tersimpan di lokasi terpisah (off-site storage), aman dari kerusakan lokal pada router.

Membedah hubungan kausalitas antara implementasi protokol keamanan dan kinerja jaringan fisik. Rifqi dkk. menggunakan pendekatan kuantitatif untuk mengukur dampak langsung dari aturan firewall Port Knocking terhadap parameter kinerja utama: Throughput, Delay (Latensi), dan Packet Loss. Teori ini didasarkan pada premis bahwa setiap penambahan aturan (rule) pada firewall akan menambah beban pemrosesan pada CPU router (overhead), yang secara teoretis dapat memperlambat laju transmisi data. Analisis performa ini krusial untuk membuktikan kelayakan implementasi teknik keamanan dalam lingkungan produksi [7]. Sementara itu, membahas dua pendekatan fundamental dalam mengelola akses port jaringan: pendekatan statis (Port Blocking) dan pendekatan dinamis (Port Knocking). Port Blocking adalah teknik keamanan paling dasar di mana administrator secara permanen menutup port tertentu agar tidak dapat diakses dari jaringan luar. Teori ini menjelaskan bahwa meskipun Port Blocking sangat aman, ia memiliki kelemahan fatal dalam hal fleksibilitas; administrator yang berada di luar jaringan tidak dapat mengakses sistem untuk pemeliharaan jika port terkunci total. Ini menciptakan dilema antara keamanan dan aksesibilitas [8].

Berfokus pada pengendalian akses jaringan berdasarkan identitas perangkat, yang direpresentasikan oleh alamat IP dan MAC Address. Maulana dan Kholiq mengangkat permasalahan akses ilegal di mana pengguna yang tidak berhak (intruder) menyusup ke dalam jaringan dengan menggunakan IP statis yang tidak terpakai atau melakukan pemindaian IP (IP Scanning). Teori IP Filtering menyatakan bahwa keamanan jaringan harus dimulai dengan validasi entitas yang terhubung. Router Mikrotik difungsikan sebagai penjaga gerbang yang memverifikasi setiap paket data terhadap daftar putih (whitelist) alamat IP yang diizinkan [9].

Kesimpulannya, teori Manajemen Akses Berbasis IP ini menekankan bahwa identifikasi adalah langkah pertama dari keamanan. Sebelum memeriksa apa yang ingin dilakukan oleh sebuah paket data (misalnya mengakses web atau database), sistem harus terlebih dahulu memvalidasi siapa (IP mana) yang mengirimkannya. Kombinasi IP Filtering untuk validasi identitas dan Port Knocking untuk validasi otorisasi menciptakan kerangka kerja keamanan yang komprehensif, sangat relevan untuk lingkungan jaringan yang melayani banyak pengguna dengan tingkat kepercayaan yang berbeda-beda. Penelitian di Taman Margasatwa Ragunan perlu membuktikan bahwa penambahan lapisan keamanan tidak merugikan kenyamanan pengguna. Teori analisis performa (Throughput, Delay, Packet Loss) adalah alat validasi utama. Relevansinya adalah untuk menjawab pertanyaan manajemen Ragunan: "Apakah sistem ini akan membuat internet kami lemot?"

Dengan menggunakan teori ini, peneliti dapat melakukan pengujian empiris di jaringan simulasi Ragunan. Mengukur latensi saat staf melakukan akses database pengunjung melalui jalur yang diproteksi Port Knocking vs jalur biasa. Hasil analisis berdasarkan teori ini akan memberikan justifikasi teknis bahwa dampaknya terhadap performa sangat minim dan dapat diabaikan (negligible). Teori ini juga relevan untuk menyetel (tuning) konfigurasi. Jika hasil analisis menunjukkan adanya delay tinggi pada tahap awal implementasi, peneliti bisa menggunakan teori ini untuk mengoptimalkan urutan rules firewall di Mikrotik Ragunan (misalnya, menempatkan rule Established/Related di posisi paling atas) untuk memperbaiki kinerja sesuai parameter teori.

Analisis Packet Loss sangat penting untuk layanan tiket elektronik Ragunan. Transaksi finansial tidak mentolerir kehilangan data. Teori ini memastikan bahwa mekanisme Port Knocking dikonfigurasi dengan presisi tinggi sehingga tidak ada paket data transaksi yang terbuang secara tidak sengaja, menjaga reliabilitas pendapatan kebun binatang. Kesimpulannya, teori ini adalah dasar evaluasi keberhasilan penelitian. Tanpa analisis performa ini, implementasi di Ragunan hanya bersifat teoretis fungsional tetapi belum tentu layak operasional. Data yang dihasilkan dari penerapan teori ini akan menjadi bukti kuat kelayakan sistem.

II. METODE PENELITIAN

Penelitian ini menggunakan pendekatan eksperimental dengan tujuan menguji efektivitas teknik Port Knocking pada perangkat Mikrotik RouterOS dalam meningkatkan keamanan jaringan. Tahap awal penelitian dimulai dengan studi literatur untuk memahami konsep dasar keamanan jaringan, prinsip kerja Port Knocking, serta karakteristik perangkat Mikrotik RouterOS. Informasi dari jurnal, buku, dan dokumentasi teknis digunakan sebagai dasar perancangan skenario implementasi. Selanjutnya, kebutuhan teknis ditetapkan meliputi konfigurasi router, struktur jaringan simulasi, perangkat lunak pendukung, serta parameter pengujian yang akan dijadikan acuan dalam evaluasi.

Peneliti merancang topologi jaringan berbasis simulator yang disesuaikan dengan kondisi operasional Taman Margasatwa Ragunan sebagai lingkungan semi publik. Mikrotik RouterOS dikonfigurasi untuk menerapkan Port Knocking pada port layanan kritikal yang menjadi target utama serangan. Skenario serangan disusun untuk mensimulasikan ancaman nyata, di antaranya percobaan akses ilegal dan brute force attack menggunakan IP eksternal. Seluruh langkah konfigurasi dicatat secara sistematis untuk memastikan replikasi dan validasi dapat dilakukan pada tahap selanjutnya.

Penelitian berfokus pada proses pengujian dan analisis hasil. Pengujian dilakukan dengan mengevaluasi kemampuan Port Knocking dalam memberikan proteksi terhadap akses tidak sah, sekaligus memastikan stabilitas koneksi jaringan tetap terjaga selama proses autentikasi. Data yang diperoleh dari simulasi dianalisis untuk menilai keberhasilan mekanisme Port Knocking dalam memblokir serangan, membuka akses hanya untuk pengguna yang memenuhi urutan ketukan port, serta memastikan tidak terjadi degradasi signifikan pada fungsi jaringan dasar. Hasil analisis digunakan untuk menarik kesimpulan mengenai efektivitas Port Knocking sebagai solusi keamanan yang efisien dan dapat diimplementasikan pada lingkungan semi publik.

III. HASIL DAN PEMBAHASAN

Penelitian dilakukan dengan mengimplementasikan mekanisme Port Knocking pada perangkat Mikrotik RouterOS menggunakan topologi jaringan simulasi yang merepresentasikan kondisi operasional Taman Margasatwa Ragunan sebagai lingkungan semi publik. Tahap implementasi diawali dengan konfigurasi firewall filter, pembuatan aturan address list, serta penentuan urutan port knocking yang harus diakses sebelum pengguna memperoleh izin untuk mengakses layanan administrasi router. Setelah konfigurasi selesai, dilakukan beberapa skenario pengujian untuk mengevaluasi efektivitas sistem dalam menghadapi akses tidak sah dan menjaga kestabilan jaringan. Hasil pengujian menunjukkan bahwa pengguna yang mencoba mengakses layanan administrasi secara langsung tanpa melakukan urutan Port Knocking tidak dapat terhubung ke router.

Seluruh paket yang masuk menuju port layanan diblokir oleh aturan firewall sehingga tidak ada akses yang berhasil dilakukan. Sebaliknya, pengguna yang melakukan urutan ketukan port sesuai konfigurasi berhasil dimasukkan ke dalam address list secara otomatis dan memperoleh hak akses dalam batas waktu tertentu. Hal ini menunjukkan bahwa mekanisme autentikasi tambahan melalui Port Knocking mampu membedakan pengguna yang sah dengan pihak yang tidak memiliki otorisasi. Pengujian juga dilakukan menggunakan simulasi brute force attack dan port scanning dari alamat IP eksternal. Berdasarkan hasil pengamatan pada log Mikrotik, seluruh percobaan akses yang tidak memenuhi urutan Port Knocking berhasil diblokir oleh firewall tanpa memberikan respons yang menunjukkan keberadaan layanan administrasi. Kondisi tersebut menunjukkan bahwa Port Knocking mampu menyembunyikan (service obfuscation) port layanan sehingga peluang keberhasilan serangan otomatis menjadi lebih kecil. Selain itu, setiap aktivitas yang terdeteksi dapat dicatat pada log sistem sehingga administrator memiliki informasi untuk melakukan pemantauan keamanan jaringan.

Dari sisi kinerja jaringan, implementasi Port Knocking tidak menunjukkan penurunan performa yang signifikan selama proses pengujian. Koneksi jaringan tetap berjalan normal untuk layanan umum, sementara proses autentikasi hanya menambah waktu yang sangat singkat sebelum akses administrasi diberikan kepada pengguna yang berhak. Hal ini menunjukkan bahwa mekanisme keamanan yang diterapkan mampu meningkatkan proteksi jaringan tanpa mengganggu fungsi utama jaringan maupun kualitas layanan kepada pengguna.

Secara keseluruhan, hasil penelitian membuktikan bahwa penerapan Port Knocking pada Mikrotik RouterOS efektif dalam meningkatkan keamanan jaringan, khususnya pada lingkungan semi publik seperti Taman Margasatwa Ragunan. Mekanisme ini mampu mencegah akses ilegal, mengurangi risiko serangan brute force dan port scanning, serta memberikan lapisan keamanan tambahan sebelum proses autentikasi dilakukan. Temuan ini juga sejalan dengan konsep defense in depth, di mana keamanan tidak hanya bergantung pada firewall, tetapi juga pada mekanisme autentikasi tersembunyi yang memperkuat perlindungan terhadap layanan kritikal. Dengan demikian, Port Knocking dapat dijadikan salah satu solusi keamanan yang sederhana, efisien, dan mudah diimplementasikan pada jaringan berbasis Mikrotik RouterOS.

Meskipun demikian, penelitian ini memiliki keterbatasan karena pengujian dilakukan menggunakan simulator jaringan yang merepresentasikan kondisi operasional Taman Margasatwa Ragunan, sehingga belum sepenuhnya menggambarkan performa sistem pada infrastruktur fisik yang sebenarnya. Oleh karena itu, hasil pengujian berpotensi berbeda ketika diimplementasikan pada kondisi nyata yang melibatkan gangguan fisik, seperti kerusakan kabel, fluktuasi daya listrik, maupun faktor lingkungan lainnya yang dapat memengaruhi kinerja jaringan.

IV. SIMPULAN

4.1 Kesimpulan

Berdasarkan hasil implementasi dan pengujian, penerapan Port Knocking pada Mikrotik RouterOS terbukti efektif dalam meningkatkan keamanan jaringan pada lingkungan semi publik. Mekanisme ini berhasil membatasi akses ke layanan administrasi router sehingga hanya pengguna yang melakukan urutan knocking yang benar yang dapat memperoleh hak akses. Pengujian juga menunjukkan bahwa percobaan akses ilegal, brute force attack, dan port scanning dapat diblokir oleh firewall, sementara layanan jaringan tetap berjalan dengan baik tanpa penurunan kinerja yang signifikan. Dengan demikian, Port Knocking dapat menjadi solusi keamanan tambahan yang sederhana, efisien, dan mudah diterapkan untuk memperkuat sistem keamanan jaringan berbasis Mikrotik RouterOS serta mengurangi risiko akses tidak sah terhadap layanan kritikal.

4.2 Saran

Penelitian selanjutnya disarankan untuk melakukan implementasi dan pengujian secara langsung pada infrastruktur jaringan fisik di Taman Margasatwa Ragunan guna memvalidasi hasil simulasi. Selain itu, mekanisme Port Knocking dapat diintegrasikan dengan sistem notifikasi real-time, seperti Telegram Bot atau email, serta dikombinasikan dengan Virtual Private Network (VPN), Intrusion Detection System (IDS), atau Intrusion Prevention System (IPS) untuk membangun sistem keamanan berlapis (defense in depth). Pengujian juga perlu diperluas pada lingkungan jaringan yang lebih kompleks dengan jumlah pengguna dan lalu lintas yang lebih besar untuk mengevaluasi kinerja serta skalabilitas sistem..

REFERENSI

[1] F. Febri and E. Hutabri, “Rancang Bangun Sistem Keamanan Jaringan Mikrotik Menggunakan Firewall Filtering Dan Port Knocking Dengan Notifikasi Telegram Pada Event Virtual,” *Comput. Sci. Ind. Eng.*, vol. 9, no. 4, 2023, doi: 10.33884/comasiejournal.v9i4.7704.

[2] R. Dwiyanto, R. Nurtantyo S, I. Kurniasari, and H. Kurniadi, “Implementasi Keamanan Jaringan Pada Mikrotik Menggunakan Teknik Port Knocking Pada Smk Al - Amien,” *J. Minfo Polgan*, vol. 14, no. 1, pp. 293–301, 2025, doi: 10.33395/jmp.v14i1.14691.

[3] F. Baso and M. Ardiansyah, “Implementasi Metode Port Knocking pada MikroTik RouterOS untuk Mendukung Keamanan Jaringan,” *J. Secur. Comput. Information, Embed. Network, Intell. Syst.*, vol. 8329, pp. 31–35, 2023, doi: 10.61220/scientist.v1i1.235.

[4] Ismanto and Aristejo, “Optimalisasi Keamanan Jaringan Menggunakan Metode Port Knocking Pada LAZIS Wahdah Jakarta,” *J. Tek. Inform.*, vol. 7, no. 1, pp. 40–48, 2021, doi: 10.51998/jti.v7i1.350.

[5] Y. Christian, “Analisis Sistem Pengamanan Akses Autentikasi Jaringan dengan Metode Port Knocking dan Action Tarpit pada Router Mikrotik,” *Telcomatics*, vol. 4, no. 1, pp. 1–6, 2019, doi: 10.37253/telcomatics.v4i1.586.

[6] S. Setyowibowo and N. Moka, “Keamanan Jaringan Hotspot Dengan Simple Port Knocking Dan Automated Backup Menggunakan Mikrotik,” *J. Ilm. Komputasi*, vol. 21, no. 4, pp. 541–552, 2022, doi: 10.32409/jikstik.21.4.3109.

[7] M. Z. Rifqi, “Implementasi Sistem Keamanan Jaringan Pada Mikrotik Rb-951 Menggunakan Metode Port Knocking,” *J. Tektro*, vol. 05, no. 02, pp. 165–173, 2021.

[8] I. P. A. A. Repi and S. Soim, “Implementasi Port Knocking, Port Blocking Pada Keamanan Jaringan Komputer Berbasis Mikrotik,” *J. Resist. (Rekayasa Sist. Komputer)*, vol. 6, no. 3, pp. 125–130, 2023, doi: 10.31598/jurnalresistor.v6i3.1463.

[9] P. D. Aplikasi Pemesanan Di *et al.*, “Analisis Dan Perancangan Sistem Penjadwalan Optimum Preventive Maintenance Machine Molding Injection Dan Blow Menggunakan Metode Relliabilty Centerd Maintenance (RCM) Analisis dan Implementasi Keamanan Jaringan Mikrotik dengan Metode IP Filtering dan Port Knockiing (Studi Kasus Barokah.Net),” vol. 19, no. 2, 2022.