

Implementasi Keamanan Jaringan Menggunakan *Port Knocking*

Network Security Implementation Using Port Knocking

Nugroho Adhi Santoso¹, Khaediar Bagus Affandi², Rifki Dwi Kurniawan³

^{1,3}Program Studi Sistem Informasi, STMIK Tegal

²Program Studi Teknik Informatika, STMIK Tegal

e-mail: nugrohoadhisantoso29@gmail.com¹, khaediarbagus@gmail.com², rifki.dk@gmail.com³

Received:
01.01.2021

Revised:
01.01.2021

Accepted:
01.01.2021

Available online:
01.01.2021

Abstrak: Teknologi informasi harus diperbarui setiap tahun karena masalah keamanan data dan informasi. Keamanan informasi menjadi semakin penting seiring dengan perubahan teknologi informasi dan masih terus berubah hingga saat ini. Serangan pada server telah sering dilakukan oleh pengguna yang ceroboh. Keamanan jaringan perlu ditingkatkan untuk mengurangi penyalahgunaan jaringan hacker. Pada penelitian ini port knocking digunakan untuk melakukan penelitian untuk pembuatan jaringan komputer yang aman. Berdasarkan hasil analisis dan pengujian implementasi sistem, dapat disimpulkan bahwa sistem dapat berfungsi secara efektif dan keamanan jaringan bawaannya dapat ditingkatkan dibandingkan dengan keamanan non-jaringan. Pasang keamanan port knock pada tempatnya. Kehadiran otentikasi yang sesuai saat mengakses adalah buktinya.

Kata kunci: *port knocking*, keamanan jaringan, jaringan komputer

Abstract: Information technology must be updated annually due to data and information security concerns. Information security has become increasingly crucial as information technology has changed and is still changing today. Attacks on the server have been made frequently by careless users. Network security needs to be improved in order to decrease hacker network abuse. In this study, port knocking was used to conduct research for the creation of a secure computer network. Based on the analysis and testing results of the system's implementation, it can be concluded that the system can function effectively and that its built-in network security can be enhanced as compared to non-network security. Put port knock security into place. The presence of suitable authentication while accessing is proof of this.

Keywords: *port knocking*, network security, computer network

1. PENDAHULUAN

Hingga saat ini perkembangan teknologi semakin meningkat. Keamanan sistem dipengaruhi oleh perkembangan ini. Oleh karena itu, pengguna aplikasi yang terhubung dengan jaringan internet perlu lebih berhati-hati terhadap penyusupan oleh pihak yang tidak berwenang. Ada banyak pengguna internet yang menjadi korban penyusupan. Salah satu penyusupan yang berhasil melibatkan situs resmi MUI, yang telah disusupi oleh peretas [1]. Malware, trojan, virus, dan pemindaian port adalah beberapa dari risiko keamanan yang sering ditemukan. Menggunakan jaringan, pemindaian port adalah metode untuk menemukan port komputer yang terbuka [2].

Jaringan komputer tidak dapat beroperasi tanpa keamanan jaringan. Jika kerentanan jaringan komputer tidak ditambal, kerugian dapat diakibatkan oleh hilangnya data atau file, kerusakan sistem server, layanan pengguna di bawah standar, atau bahkan hilangnya aset institusional yang tak ternilai harganya. Karena bahaya penyerangan yang semakin canggih dan bervariasi, keamanan jaringan menjadi masalah yang sangat penting untuk diperhatikan. Ini terutama benar ketika jaringan lokal terhubung ke internet. Ancaman yang tidak bisa dihindari antara lain *Distributed Denial of Service* (DDoS), serangan hacker, virus, dan trojan [3].

Port knocking adalah metode yang digunakan untuk membuka akses ke port tertentu yang telah diblokir oleh Firewall pada perangkat jaringan dengan mengirimkan paket atau koneksi tertentu [4]. Kelebihan port knocking dengan firewall adalah walaupun semua port tertutup, mereka memiliki hak akses dan mengetahui knocking untuk membuka port sehingga user dapat selalu menggunakan port yang telah dibuka. Implementasi *port knocking* yang terdapat tidak dapat di skalakandalam penyebaran penyedia layanan karena pemakaian rahasia bersama urutan knocking kurang rentan terhadap serbuan replay serta *brute force* apabila usianya lebih pendek. Implementasi *port knocking* bersumber pada sertifikat x509 bertujuan guna menjadi sangat skalabel. Akan tetapi, *port knocking* sendiri mempunyai beberapa kelemahan seperti misalnya *TCP replay attacks*, *port scan*, ketidakjelasan keamanan serta pengiriman paket tidak cocok karena latensi jaringan melakukan pengelolaan aset tanpa memperhitungkan value dari aset dapat mengakibatkan kerugian bagi toko [5].

Peneliti memanfaatkan proses *port knocking*, yaitu sistem keamanan jaringan yang dirancang khusus untuk sebuah jaringan, untuk menangkal serangan terhadap *port* pada sistem jaringan komputer. Intinya, menutup semua *port* yang terbuka adalah cara kerja *port knocking*. Selain itu, hanya pengguna tertentu yang harus menyentuh terlebih dahulu yang dapat mengakses *port* yang telah dikonfigurasi [6].

2. TINJAUAN PUSTAKA

Port Knocking

Gagasan di balik *port knocking* adalah menyembunyikan layanan dari jarak jauh di belakang firewall dan hanya mengizinkan akses ke *port* tersebut ketika klien telah berhasil diautentikasi dengan firewall. Ini dapat melindungi server dari serangan zero-day dan mencegah pemindai mengetahui layanan apa yang saat ini tersedia [1].

Keamanan Jaringan

Praktik mencegah dan mengenali penggunaan jaringan komputer yang tidak sah dikenal sebagai keamanan jaringan komputer. Tujuan dari keamanan jaringan komputer adalah untuk meramalkan bahaya pada jaringan komputer berupa ancaman fisik dan logis yang dapat mengganggu operasi jaringan komputer secara langsung atau tidak sengaja. Selain itu, untuk melindungi data sistem komputer dari berbagai risiko [7].

Firewall

Sistem Firewall adalah mekanisme yang diterapkan pada perangkat keras dan perangkat lunak dengan tujuan melindungi, membatasi, memfilter, atau bahkan menolak aktivitas suatu segmen di jaringan lokal ke jaringan eksternal yang tidak berada dalam cakupannya. Firewall bertanggung jawab untuk memastikan bahwa tidak ada yang ditambahkan di luar rentang yang diizinkan [8].

3. METODE

3.1. *Literatur Review*

Sebuah studi sekunder yang disebut tinjauan literatur sistematis (SLR) digunakan untuk memetakan, mengidentifikasi, menilai secara kritis, meringkas, dan membedakan temuan penelitian utama pada topik penelitian tertentu. Dengan melakukan tinjauan literatur berdasarkan penelitian sebelumnya yang relevan, SLR telah muncul sebagai norma untuk menemukan solusi. SLR digunakan untuk mensintesis penelitian sebelumnya, mengidentifikasi kesenjangan pengetahuan antara penelitian ini dan penelitian saat ini, mengembangkan laporan atau sintesis yang koheren, dan membuat kerangka kerja penelitian [9]. Pengumpulan data adalah di mana data dari studi dikumpulkan. Tujuan dari tinjauan literatur ini dalam Studi adalah untuk memahami topik penelitian keamanan jaringan menggunakan *port knocking*. Penelitian akan diteliti dari sejumlah makalah yang diterbitkan di *Google Scholar*, *IEEE*, *SpringerLink*, *ResearchGate* dan *IECE* antara tahun 2017 dan 2022 dalam bentuk jurnal atau konferensi. Dokumen yang dicari dalam bahasa Indonesia dan dalam bahasa Inggris. Kata kunci yang digunakan adalah "*port knocking*", "*cybersecurity*" [10].

3.2. *Pertanyaan Penelitian*

Tujuan dari tinjauan literatur dalam penelitian ini adalah untuk memahami topik penelitian, metode dan fungsi yang digunakan dalam analisis keamanan jaringan. mendapatkan hasil yang komprehensif, penelitian ini menggunakan sejumlah makalah yang dipublikasikan di jurnal database ternama seperti *IEEE Xplore*, *ScienceDirect*, *Google Scholar* dari tahun 2017 hingga 2022. Mereka dikelompokkan berdasarkan pertanyaan penelitian seperti yang ditunjukkan pada pemaparan di bawah ini.:

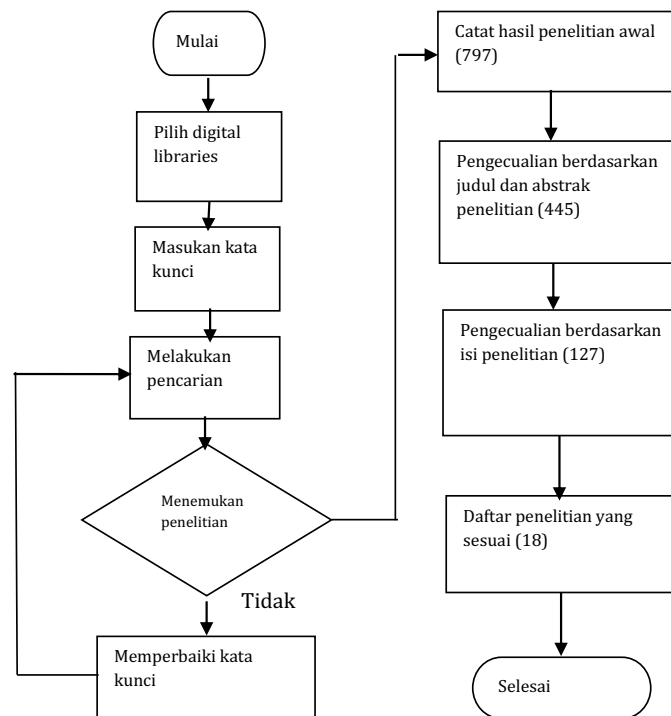
RQ1: Apa jenis metode yang di gunakan dalam sistem keamanan jaringan? Penting untuk mengidentifikasinya agar penelitian ini dapat menampilkan informasi tentang jenis dan karakteristik metode eksperimen yang dilakukan sehingga peneliti memiliki gambaran tentang bagaimana melakukan penelitian dengan metode tersebut metode yang relevan untuk penelitian masa depan.

RQ2: Apakah sistem keamanan jaringan menggunakan alat tertentu? Alat uji sering digunakan untuk pengujian, sehingga dengan mengetahui alat yang digunakan dapat mempermudah dalam mengaplikasikan alat untuk pembelajaran selanjutnya.

RQ3: Apakah sistem keamanan jaringan telah diterapkan pada kasus nyata? Berbeda dengan pengujian yang diberikan, pengujian pada kasus nyata dapat menunjukkan bahwa metode atau alat dapat menjanjikan hasil yang lebih nyata dalam sistem keamanan jaringan.

3.3. Seleksi Study

Selama pencarian kata kunci awal dan berdasarkan tahun publikasi, yaitu 2017-2022, jumlah teks yang diperoleh adalah 797 teks. Sebanyak 797 judul dari literatur akan ditinjau dan ditentukan berdasarkan kriteria inklusi dan kriteria eksklusi. Selama proses seleksi dengan kriteria inklusi, diperoleh literatur, kemudian 72 literatur tersebut dipisahkan untuk dianalisis kembali sesuai dengan kriteria eksklusi, subjek dan kemungkinan judul yang terkait. Pada hasil analisis ini diperoleh publikasi yang cocok berdasarkan kriteria eksklusi, topik relevan dan judul, setelah mendapatkan publikasi, dilakukan langkah seleksi ulang dengan bacaan dari masing-masing publikasi termasuk abstrak, kata kunci dan kesimpulan. Dari tahap tersebut dihasilkan 28 literatur yang terkumpul yang dinilai sesuai dan dijadikan sebagai bahan studi literatur.



Gambar 1. Flowchart Proses Pencarian

4. HASIL DAN PEMBAHASAN

Dari hasil penelusuran publikasi ilmiah dalam daftar *database* digital terpilih, terpilih beberapa publikasi ilmiah yang dapat dijadikan sumber untuk menjawab pertanyaan penelitian yang dirumuskan oleh penulis, ringkasan hasil evaluasi dipaparkan pada penjelasan berikut.

RQ1 : Apa jenis metode yang di gunakan dalam sistem keamanan jaringan?

Metode port knocking digunakan untuk menetapkan parameter sedemikian rupa sehingga peralatan komputer ini tidak memiliki port komunikasi terbuka yang bebas untuk dimasuki, tetapi masih dapat dijangkau dari luar untuk mencegah serangan yang dilakukan dalam keadaan port terbuka [5].

Metode port Knocking memiliki kelebihan, dimana meskipun port yang ada ditutup, pengguna tetap dapat mengakses port tersebut dengan metode penyadapan, port mana yang dapat diakses oleh pengguna jika pengguna mengetahui metode penyadapan, Metode ini merupakan

metode yang sangat efisien untuk melindungi sistem jaringan dan banyak digunakan untuk memastikan keamanan jaringan, namun meskipun sistem ini cukup efisien, tidak jarang pemblokiran firewall menjadi tidak fleksibel ketika harus terhubung dengan seseorang ke jaringan. , firewall tidak mengizinkannya karena mungkin berada di area yang tidak diizinkan oleh firewall, Port Knocking merupakan metode atau cara komunikasi dua arah (client dan server) dimana metode ini diimplementasikan pada sistem dengan port tertutup. [11]

Dengan mengirimkan paket atau koneksi tertentu, teknik yang dikenal sebagai *port knocking* memungkinkan perangkat jaringan untuk mendapatkan akses ke beberapa port yang telah dibatasi oleh *Firewall* [12].

Hasil dari penerapan metode *Port Knocking* pada sebuah sistem di jaringan komputer yaitu sistem akan menolak apabila aktivitas login pada sistem tidak atau salah mengirimkan parameter tambahan, selain itu admin jaringan dapat mengetahui aktivitas di sistem jaringan jika ada seseorang dari luar gagal saat akan mengakses sistem melalui port tertentu, sehingga dapat dilakukan tindakan sesuai dengan kebutuhan keamanan sistem [13], Fungsi penyadapan port adalah untuk menutup semua port yang ada dan hanya pengguna tertentu yang dapat mengakses port yang ditentukan dengan terlebih dahulu mengetuk.

Cara paling sederhana untuk memperbaikinya adalah dengan menyebarkan Port Knocking dan HoneyPot di jaringan server. Teknik ini digunakan untuk membantu mengelola server (*Linux* dan *Unix*) dan memantau jaringan dengan menembus dan mencegah akses ke port pada server yang ada di dalam jaringan. Di mana *Port Knocking* dapat mengelola layanan terbuka dan tertutup *port* [14].

Dibandingkan dengan jaringan yang tidak menggunakan keamanan port knocking, temuan analisis keamanan jaringan dan uji implementasi *port knocking* menunjukkan bahwa pendekatan keamanan port knocking dapat beroperasi secara optimal dan dapat meningkatkan keamanan jaringan [15].

RQ2 : Apakah sistem keamanan jaringan menggunakan alat tertentu?

Penelitian ini menerapkan simple *port knocking* untuk meningkatkan keamanan dari serangan *brute force mikrotik*, hasil dari penelitian ini yaitu tabel perbandingan keamanan mikrotik dengan menggunakan simple *port knocking* dan tanpa menggunakan mikrotik [5] [12].

Fitur *firewall* pada router Mikrotik berfungsi untuk mengamankannya dengan cara memblokir atau menangkap sebuah paket sebelum masuk, melewati, atau meninggalkan router [8], Teknologi firewall sendiri berguna untuk mengontrol semua komunikasi yang mencoba masuk atau keluar, dimana port yang tidak penting atau tidak digunakan dapat diblokir (ditutup) dan port yang penting dan berbahaya juga dapat diblokir (ditutup) oleh firewall. , jadi hanya pihak yang diizinkan masuk melalui pelabuhan ini, Oleh karena itu, peran firewall sangat penting dalam sistem jaringan, di mana peran firewall itu sendiri adalah memblokir port-port sistem jaringan yang terbuka secara bebas, prinsip operasi firewall adalah menutup semua port secara independen, bahkan jika pengguna memiliki izin untuk menggunakan port tersebut. [11].

Sesuai dengan aturan yang telah ditetapkan dan disepakati bersama, router Mikrotik digunakan untuk mengontrol lalu lintas data internet dan menyaring berbagai macam serangan jaringan yang dapat menghambat konektivitas jaringan komputer [14] [16].

RQ3 : Apakah sistem keamanan jaringan telah diterapkan pada kasus nyata?

Pengujian dalam situasi aktual, berbeda dengan pengujian yang ditentukan, mungkin menunjukkan bahwa metode atau instrumen dapat menjamin hasil yang lebih konkret dalam sistem keamanan jaringan. Salah satu contoh nyata dari tujuan penelitian adalah untuk menganalisis simulasi keamanan jaringan yang disesuaikan dengan arsitektur jaringan di Taman Pintar Yogyakarta dengan menggunakan berbagai kemampuan Mikrotik, seperti firewall dan fitur peningkatan keamanan jaringan lainnya [17] [5].

Peneliti dapat membantu administrator mengamankan Routerboard Mikrotik pada sistem jaringan komputer SMK N 1 Sumbawa Besar dengan menggunakan pendekatan Port Knocking yang dapat membantu meningkatkan keamanan jaringan [6].

Contoh nyata lainnya adalah studi yang menghasilkan model yang dapat digunakan sebagai panduan untuk membuat dan meningkatkan keamanan akses jaringan komputer nirkabel pada

jaringan kampus STMIK Mataram [16] [18].

Banyaknya perusahaan, kantor dan institusi yang sudah menggunakan internet untuk mengakses berbagai informasi yang diperlukan seperti LKP SURYA KOMPUTER, Aktivitas jaringan LKP Surya Computer bisa tergolong tinggi, karena ada satu hal yang saat ini menghambat pembelajaran dan akses banyak pengguna yaitu kurangnya keamanan jaringan pada router Mikrotik, karena ada penyusup yang masuk. mengubah pengaturan router Mikrotik dan menyebabkan masalah keamanan jaringan yang cukup fatal sehingga membutuhkan keamanan jaringan yaitu Port Knocking [19].

5. KESIMPULAN

Pada penelitian ini akan dikembangkan sistem keamanan jaringan yang melindungi router Mikrotik menggunakan metode port knocking, yang berfungsi sebagai alternatif untuk menjaga keamanan jaringan informasi, mencegah penyerang mengakses router Mikrotik, dan administrator dapat menentukan siapa yang memiliki akses ke pelabuhan-pelabuhan tertentu.

Dengan menggunakan pendekatan *Port Knocking* untuk menegaskan keamanan jaringan, dimungkinkan untuk mengurangi insiden pihak yang tidak bertanggung jawab menyalahgunakan akses router.

Sesuai dengan perancangan dan pengembangan program *port knocking* maka dapat ditarik beberapa kesimpulan antara lain program *port knocking* dapat menentukan port mana yang dapat di akses client, program *port knocking* dapat menentukan port mana yang tidak dapat di akses client, jika client melakukan tidak memiliki akses, tidak dapat berbagi file atau berkomunikasi dengan server. Membuat aplikasi yang menggabungkan utilitas *port knocker* untuk terhubung ke port yang dilarang oleh *firewall* adalah saran untuk pengembangan.

DAFTAR PUSTAKA

- [1] A. Amarudin, "Desain Keamanan Jaringan Pada Mikrotik Router OS Menggunakan Metode Port Knocking," *J. Teknoinfo*, vol. 12, no. 2, p. 72, 2018, doi: 10.33365/jti.v12i2.121.
- [2] T. Brades and Irwansyah, "Pemanfaatan Metode Port Knocking Dan Blocking Untuk Keamanan Jaringan Bpkad Provinsi Sumsel," pp. 99–107, 2022.
- [3] A. Saputro, N. Saputro, H. Wijayanto, and P. S. Informatika, "Metode Demilitarized Zone Dan Port Knocking Untuk Demilitarized Zone and Port Knocking Methods for Computer," *Metode*, vol. 3, no. 2, pp. 22–27, 2020, [Online]. Available: <https://scholar.archive.org/work/vuzz46kj7zb3rpanfhuilpg3aq/access/wayback/http://ejournal.uin-suka.ac.id/saintek/cybersecurity/article/download/2150/1801>
- [4] S. J. I. I. Devie Ryana Suchendra1, Alfian Fitra Rahman2, "Penerapan sistem pengamanan port pada layanan jaringan menggunakan port knocking," *J. Lpkia*, vol. 10, no. 2, pp. 45–50, 2017.
- [5] P. Riska, P. Sugiartawan, and I. Wiratama, "Sistem Keamanan Jaringan Komputer Dan Data Dengan Menggunakan Metode Port Knocking," *J. Sist. Inf. dan Komput. Terap. Indones.*, vol. 1, no. 2, pp. 53–64, 2018, doi: 10.33173/jsikti.12.
- [6] M. Julkarnain and A. J. Afahar, "Implementasi Port Knocking Untuk Keamanan Jaringan Smkn 1 Sumbawa Besar," *J. Inform. Teknol. dan Sains*, vol. 3, no. 2, pp. 326–335, 2021, [Online]. Available: <http://www.jurnal.uts.ac.id/index.php/JINTEKS/article/view/1016>
- [7] M. Akbar, T. A. Agung, M. I. I, and A. Fauzi, "Analisis Keamanan Jaringan Komputer Pada Sekolah Menengah Atas Negeri 04 Bandung," *J. Nas. Komputasi dan Teknol. Inf.*, vol. 4, no. 4, pp. 258–264, 2021, doi: 10.32672/jnkti.v4i4.3106.
- [8] S. P. Putra and Y. Ramdhani, "Memanfaatkan Fitur Firewall Rules Pada Mikrotik Untuk Keamanan Jaringan Di Hotel Lenora Bandung," *eProsiding Tek. Inform.*, vol. 2, no. 1, pp. 122–126, 2021, [Online]. Available: <https://eprosiding.ars.ac.id/index.php/pti>
- [9] F. Rozi, "Systematic Literature Review pada Analisis Prediktif dengan IoT: Tren Riset, Metode, dan Arsitektur," *J. Sist. Cerdas*, vol. 3, no. 1, pp. 43–53, 2020, doi: 10.37396/jsc.v3i1.53.
- [10] Z. Ilma Rimbarawa, E. Kholisoh, and Z. Putri Rahmayani, "Systematic Literature Review: Permasalahan Ransomware pada Aplikasi Berbasis Cloud | INTECH," *J. Inform. dan Teknol.*, vol. 2, no. 2, pp. 19–22, 2021, [Online]. Available: <https://journal.unbara.ac.id/index.php/INTECH/article/view/877>
- [11] M. Z. Rifqi and M. Syahroni, "IMPLEMENTASI SISTEM KEAMANAN JARINGAN PADA MIKROTIK RB-951 MENGGUNAKAN METODE PORT KNOCKING," vol. 05, no. 02, pp. 165–173, 2021.
- [12] N. Firdaus and A. Fitriawan, "Implementasi Keamanan Mikrotik Menggunakan Metode Simple Port

- Knocking Pada Sman 1 Ngantang,” *J. Teknol. Inf.*, vol. 9, pp. 133–140, 2018.
- [13] D. Novianto, L. Tommy, and Y. Setiawan Japriadi, “Implementation of a Network Security System Using the Simple Port Knocking Method on a Mikrotik-Based Router Implementasi Sistem Keamanan Jaringan Menggunakan Metode Simple Port Knocking Pada Router Berbasis Mikrotik,” *J. Kom.*, vol. 1, no. 2, pp. 407–417, 2021, [Online]. Available: <https://doi.org/10.53697/jkomitek.v1i2>
- [14] R. Dwi and Y. Prakoso, “Implementasi Low Interaction HoneyPot Dan Port Knocking Untuk Meningkatkan,” vol. 02, no. 01, pp. 16–23, 2022.
- [15] R. Albar and R. O. Putra, “SNIFFING DAN IMPLEMENTASI KEAMANAN JARINGAN NETWORK SECURITY ANALYSIS USING THE METHOD SNIFFING AND IMPLEMENTATION OF NETWORK SECURITY ON MICROTIC ROUTER OS V6 . 48 . 3 USING PORT KNOCKING METHOD,” vol. 8, no. 1, pp. 1–11, 2022.
- [16] S. Aji, A. Fadlil, and I. Riadi, “Pengembangan Sistem Pengaman Jaringan Komputer Berdasarkan Analisis Forensik Jaringan,” *J. Ilm. Tek. Elektro Komput. dan Inform.*, vol. 3, no. 1, p. 11, 2017, doi: 10.26555/jiteki.v3i1.5665.
- [17] E. S. R. O. B. Langobelen, Y. Rachmawati, and C. Iswahyudi, “Analisis Dan Optimasi Dari Simulasi Keamanan Jaringan Menggunakan Firewall Mikrotik Studi Kasus Di Taman Pintar Yogyakarta,” *J. JARKOM*, vol. 7, no. 2, pp. 95–102, 2019.
- [18] L. D. Samsumar and K. Gunawan, “Analisis Dan Evaluasi Tingkat Keamanan Jaringan Komputer Nirkabel (Wireless Lan); Studi Kasus Di Kampus Stmik Mataram,” *J. Ilm. Teknol. Infomasi Terap.*, vol. 4, no. 1, pp. 73–82, 2017, doi: 10.33197/jitter.vol4.iss1.2017.152.
- [19] W. F. Fatoni *et al.*, “Jurnal Mahasiswa Ilmu Komputer (JMIK) DENGAN METODE PORT KNOCKING PADA Jurnal Mahasiswa Ilmu Komputer (JMIK),” vol. 03, no. 01, 2022.