Jurnal Ilmiah Teknik Informatika dan Komunikasi
Volume. 5 Nomor. 1 Maret 2025
e-ISSN : 2827-7945; p-ISSN : 2827-8127, Hal. 128-138
DOI: https://doi.org/10.55606/juitik.v5i1.1138
Available online at: https://journal.sinov.id/index.php/juitik

Penggunaan Metode Port Knocking untuk Meningkatkan Sistem Keamanan Jaringan Komputer

Ardian Fachreza
Jurusan Teknik Informatika, Fakultas Teknik, Universitas Wahid Hasyim

Jl. Menoreh Tengah X/19, Sampangan, Semarang 50236.
Email : ardian.fachreza@unwahas.ac.id

Abstract. *The advancement of communication and information technology demands improved computer network security to protect data from various threats such as hacker attacks and DDoS that exploit open ports. A strong security system is crucial because computer networks are vulnerable to eavesdropping and data manipulation during transmission. This research highlights the use of the Port Knocking method as an effective solution to enhance computer network security. The research employs a qualitative descriptive approach with a literature review. The author analyzes and concludes the effectiveness of port knocking in improving network security. The results show that the port knocking method effectively increases network security by closing unused ports and only allowing access to authorized users. Implementation of port knocking on Mikrotik routers successfully reduces the risk of brute force attacks and intrusions that can disrupt network connectivity. A case study at LKP Surya Computer demonstrates that this method can strengthen network security and prevent unauthorized access that could potentially damage router configurations.*

Keywords: *Firewall, Network Security, Mikrotik, Port Knocking, System.*

Abstrak. Perkembangan teknologi komunikasi dan informasi menuntut peningkatan keamanan jaringan komputer untuk melindungi data dari berbagai ancaman seperti serangan hacker dan DDoS yang memanfaatkan port terbuka. Sistem keamanan yang kuat sangat penting karena jaringan komputer rentan terhadap penyadapan dan manipulasi data selama proses pengiriman. Penelitian ini mengangkat penggunaan metode Port Knocking sebagai solusi untuk meningkatkan keamanan jaringan komputer secara efektif. Penelitian ini menggunakan metode kualitatif deskriptif dengan studi pustaka. Penulis menganalisis dan menyimpulkan efektivitas port knocking dalam meningkatkan keamanan jaringan komputer. Hasil penelitian ini menunjukkan bahwa metode port knocking efektif meningkatkan keamanan jaringan dengan menutup port yang tidak digunakan dan hanya mengizinkan akses pengguna yang sah. Implementasi port knocking pada router Mikrotik berhasil mengurangi risiko serangan brute force dan penyusupan yang dapat mengganggu konektivitas jaringan. Studi kasus di LKP Surya Computer membuktikan bahwa penerapan metode ini dapat memperkuat sistem keamanan jaringan dan mencegah akses tidak sah yang berpotensi merusak pengaturan router.

Kata Kunci: Firewall, Keamanan Jaringan, Mikrotik, Port Knocking, Sistem.

1. LATAR BELAKANG

Teknologi yang berkembang dari era ke era semakin menunjukkan perubahan kearah yang lebih maju, teknologi saat ini khususnya pada bidang komunikasi dan informasi yang semakin berkembang pesat tentunya tidak terlepas dari adanya jaringan yang memiliki peranan dalam menghubungkan perangkat sehingga penggunanya dapat memberikan informasi atau data dalam waktu yang singkat tanpa adanya batasan wilayah. Adanya jaringan ini dapat menghasilkan setiap device yang terkoneksi dapat bertukar data atau informasi yang dimiliki oleh masing-masing pengguna device. Sehingga peranan jaringan pada device ini tentunya sangat utama bagi suatu organisasi baik organisasi komersil, lembaga pendidikan, pemerintah maupun penggunaan secara pribadi (Kusuma, 2021).

Received: Januari 15, 2025; Revised: Februari 28, 2025; Accepted: Maret 25, 2025; Published: Maret 30, 2025;

Dengan adanya pertukaran data yang terjadi sangat mudah diantara deviice, maka sangat diperlukan hadirnya sistem keamanan pada jaringan device atau komputer pengguna, maka dari itu Computer Network Security yang terhubung dengan keamanan data perlu dilakukan peningkatan sistem untuk dapat melindungi data atau informasi dari berbagai ancaman. Ancaman-ancaman tersebut dapat menyerang siapapun baik instansi, perusahaan, sekalipun lembaga pemerintahan. Proses penyerangan terhadap jaringan komputer dapat dilaksanakan melalui celah atau port-port komputer yang terbuka, sehingga pihak-pihak yang tidak bertanggung jawab tersebut dapat mengakses dan mengendalikan port yang telah mereka kuasai (Yudi Mulyanto & Afahar, 2021).

Kondisi ini tentunya dapat mengakibatkan tidak dapat berjalan Jaringan komputer tanpa dilengkapi dengan keamanan jaringan. Apabila keamanan jaringan komputer tidak ditangani dengan baik maka akan mengakibatkan munculnya kerugian seperti kehilangan data atau informasi, rusaknya sistem server, pengguna layanan yang berada di bawah standar bahkan dapat mengakibatkan hilangnya aset institusional yang berharga seperti baru-baru ini terjadi pada lembaga Kominfo Indonesia. Ancaman yang dapat terjadi tanpa adanya sistem kemanan jaringan komputer seiring berjalannya waktu semakin variatif, ini menjadi titik balik agar sistem keamanan jaringan komputer diperhatikan terutama pada jaringan lokal yang terinisiasi dengan internet. Ancaman-ancaman yang sulit untuk dihindari dapat berupa Distributed Denial of Service (DDoS), serangan hacker, virus, dan trojan (Saputro et al., 2020)

Jaringan Komputer diartikan sebagai sekumpulan komputer yang terinisiasi satu sama lain yang memiliki prosedur komunikasi yang dilakukan melalui media sehingga proses penyampaian informasi, program, dan pengguna perangkat pelengkap dapat dilakukan. Dalam suatu jaringan komputer terdapat komputer, perangkat jaringan, software yang terhubung satu sama lain sehingga dapat beroperasi dalam ruang lingkup yang bisa disebut juga dengan jaringan (Saputro, Saputro, & Wijayanto, 2020).

Canggih perkembangan teknologi informasi yang ada di dunia dari masa ke masa menjadi titik perkembangan teknologi informasi yang semakin maju. Perkembangan ini tentunya dapat memberikan kemudahan bagi setiap penggunanya khususnya dalam aktivitas komunikasi (Jamalul'ain & Nurdiawan, 2022). Salah satu kecanggihan yang ada dalam jaringan komputer ialah TCP/IP (Transmission Control Protocol/Internet Protocol) yang memiliki fungsi sebagai standar komunikasi yang bersifat data untuk bertukar informasi antara berbagai device dalam suatu jaringan internet yang dapat digunakan oleh user. Tipe protokol ini sudah menjadi jenis protokol yang paling banyak digunakan oleh user namun protokol ini

tidak mampu berdiri sendiri sebab telah menjadi bagian dari komponen protocol suite (Mardiansyah et al., 2021).

Penggunaan jaringan internet saat ini telah mencapai miliaran pengguna diseluruh dunia, maka dari itu penggunaan sistem keamanan jaringan harus diperkuat salah satunya dengan menggunakan sistem protokol kontrol transmisi standar globalb(TCP / IP) untuk melindungi proses penerimaan dan pengiriman data atau informasi (Syahputra & WIjaya, 2022). Port dalam protokol TCP atau UDP, sebuah komponen dari lapisan Transport OSI, adalah port yang digunakan untuk komunikasi (Albar & Putra, 2020) Keamanan jaringan menjadi penting dan harus selalu jadi perhatian, baik Local Area Network (LAN) maupun jaringan Nirkabel atau wireless yang terhubung ke internet pada dasarnya tidak aman dan selalu rentan terhadap peretasan. Karena data harus melewati beberapa terminal untuk mencapai tujuannya, hal ini menciptakan kemungkinan bagi pengguna lain yang tidak bertanggung jawab untuk mengubah, mengganti, merusak, atau bahkan mencuri data (Attacker) (Albar & Putra, 2022)

Keamanan jaringan komputer sangat memiliki peran yang krusial dalam komponen jaringan secara menyeluruh, namun fakta masalah keamanan jaringan sering kali disepelekan, sehingga admistrato cendrung hanya berusaha menggunakan pertahanan terbaik sejauh ini, seperti firewall dan sistem deteksi intrusi (IDS) (Suryono & Chandra, 2022). Ketika data dikirimkan, akan melalui beberapa terminal sebelum mencapai tujuannya, hal ini memberi peluang penyadapan dan pengubahan data oleh pengguna lain yang tidak bertanggung jawab (Nurnaningsih & Anniar, 2022).

Mayoritas cracker menggunakan port terbuka sistem untuk menyerang sistem jaringan. Serangan Dos atau ddos, yang tertuju pada host atau komputer target dengan sejumlah besar paket yang datang dari berbagai host, adalah ilustrasi dari jenis serangan ini. Cracker perlu memahami port yang terbuka dan target agar serangan ini berhasil. Penyerang dalam melakukan aksinya akan melalui proses penyerangan melalui identifikasi komputer target atau yang dikenal dengan tahap port scanning, hal ini dilakukan penyerang untuk memperoleh data ataupun informasi yang ditargetkan melalui port yang diberikan akses pada mesin pencarian (Novianto et al., 2021).

Berdasarkan penjelasan mengenai penggunaan metode port knocking dalam menjaga sistem keamanan jaringan komputer maka penulis melakukan aktivitas penelitian dengan judul "Penggunaan Metode Port Knocking Untuk Meningkatkan Sistem Keamanan Jaringan Komputer".

2. KAJIAN TEORITIS

Metode Port Knocking

Menurut Nugroho, Port Knocking diartikan sebagai layanan yang tersembunyi dibalik firewall dan memiliki jarak yang jauh yang dapat memberikan sinyal akses bagi port yang usernya telah terautentifikasi pada firewall tersebut. Hal ini digunakan untuk melindungi dan mencegah pemindaian pada server untuk mengetahui layanan yang tersedia dari ancaman zero-day (Santoso et al., 2022). Dilain kesempatan menurut Paradika Dwi metode Port Knocking didefinisikan sebagai pembaharuan pada bidang teknologi yang dapat digunakan sebagai penjaga bagi setiap port TCP tetap tidak memberikan akses sampai user melewati proses autentikasi melalui port knocking urutan. Sistem ini tidak akan membiarkan port terbuka tanpa adanya proses autentikasi yang berhasil, sehingga dapat mencegah server dimasuki oleh pemindaian port yang membahayakan. Apabila urutan ketukan telah diverifikasi dengan valid oleh sistem maka port TCP akan melakukan koneksi standar bagi pelayanan yang telah ditentukan sebelumnya (Oktaviansyah, 2022).

Port Knocking didefinisikan menjadi satu sistem autentikasi yang dapat melakukan kerjanya secara khusus pada jaringan komputer. Metode port knocking memiliki ide dasar yang telah lama dirancang namun pada 2003 baru direalisasikan. Hakikat port knocking merupakan salah satu komunikasi yang terjalin dua arah pada komputer, yang mana data maupun informasi dapat dikirimkan melalui encode yang diteruskan dalam bentuk usaha koneksi pada port dengan urutan yang ada. Usaha dalam melakukan koneksi inilah yang disebut dengan ketukan. Port knocking memiliki mekanisme kerja melalui file log yang kemudian di firewall digunakan untuk memahami suatu usaha koneksi yang dilakukan suatu host atau tidak (Mulyanto, 2019).

Berdasarkan pendapat tersebut dapat disimpulkan bahwasanya port knocking merupakan suatu layanan yang dapat digunakan untuk menjaga aktivitas yang tidak diketahui untuk mengakses port yang ada pada jaringan komputer sehingga dapat meningkatkan keamanan sistem jaringan dari ancaman-ancaman yang membahayakan. Metode port knocking juga memiliki kelebihan diantaranya ialah adanya koneksi dengan firewall dapat menutup semua akses port, namun user tetap dapat menerima hak akses dan proses knocking untuk membuka port dengan memanfaatkan port-port yang telah terbuka. Realisasi yang digunakan oleh metode port knocking tidak dapat diskalakan dalam bentuk penyedia layanan sebagai penggunaan bersifat rahasia berdasarkan urutan knocking yang tidak rentan pada serbuan replay serta brute force jika masa penggunaannya cendrung pendek. Pengaplikasian port knocking yang diacukan pada sertifikat ×509 memiliki tujuan agar jaringan dapat skalabel. Namun penggunaan metode port knocking juga memiliki kelemahan seperti adanya TCP replay

attacks, adanya ketidakjelasan keamanan dalam mengirimkan pesan, dan port scan sehingga latensi jaringan yang digunakan pada pengelolaan aset tanpa adanya perencanaan value akan menyebabkan kerugian bagi pihak terkait (Riska et al., 2018).

Jaringan Komputer

Menurut pendapat yang disampaikan oleh Kriston jaringan komputer diartikan sebagai gabungan stasiun komunikasi yang menjadi bagian dari dua komputer atau lebih dengan koneksi yang tersedia. Jaringan komputer diadakan dengan fungsi dapat menjamin proses penyampaian informasi atau data yang diberikan oleh pengirim sampai kepada penerima dengan akurat dan tepat. Sehingga jaringan komputer dapat memberikan kemudahan bagi penggunanya untuk berkomunikasi satu sama lain. Tidak hanya itu jaringan komputer juga diperlukan agar data yang ada dapat terintergrasi pada komputer pengguna lainnya sehingga penyampaian data dapat relevan.

Ancaman yang dapat terjadi pada sistem jaringan komputer dalam bentuk penyerangan baik secara fisik maupun logika, dapat terjadi dalam beberapa bentuk berikut diantaranya ialah:(Suryono & Chandra, 2022)

- Sniffer, merupakan suatu penyerangan yang terjadi pada peralatan yang sedang mengawasi proses yang terjadi.
- Spoofing, diartikan sebagai bentuk tiruan komputer atau dalam hal ini dapat digunakan untuk memalsukan identitas atau mendapatkan alamat IP.
- Phreaking, merupakan bentuk penyerang perilaku sistem agar keamanan yang ada dapat dilemahkan.
- Remote Attack, ialah berbagai macam bentuk ancaman yang terjadi pada mesin sehingga mesin tersebut sulit untuk dikontrol yang dapat dilakukan dengan jarak yang relatif jauh diluar sistem jaringan yang dimiliki atau media transmisi yang ada.
- Hole, ialah suatu keadaan dimana hardware dan software tidak dapat diakses oleh penggunanya.

Jaringan komputer dapat diklasifikasikan menjadi dua bagian berdasarkan fungsinya, yakni:

- Jaringan peer-to-peer (P2P) atau point-to-point

  Komputer memiliki kesetaraan dalam melakukan interaksi dengan jaringan yang sama, sehingga tidak ada jaringan yang terlalu tinggi atau rendah sebab semuanya memiliki posisi yang sama. Hal ini menyebabkan setiap komputer yang ada pada jaringan akan terkoneksi dan membagi penggunaan perangkat keras maupun lunak.
- Jaringan client-server

Pada komputer jaringan ini memiliki fungsi untuk mengatur segala fasilitas yang terdapat pada jaringan komputer, misalnya pada aspek komunikasi, penggunaan perangkat lunak dan perangkat keras, serta pengontrolan jaringan, maka dari itu jaringan komputer ini disebut juga dengan server, sedangkan seluruh komputer lain disebut dengan client.

Sistem keamanan jaringan komputer memberikan sejumlah manfaat penting, antara lain mendorong *resource sharing* yang memudahkan akses data jarak jauh seolah-olah berada di lokasi yang sama, meningkatkan reliabilitas data melalui sistem backup antar komputer dalam jaringan, serta lebih hemat biaya karena penggunaan komputer pribadi yang terhubung dalam jaringan lebih efisien dibandingkan investasi pada komputer besar dengan rasio harga dan kinerja yang kurang seimbang.

- Ancaman Terhadap Jaringan Komputer

Sistem keamanan yang ada dalam suatu jaringan komputer menjadi permasalahan bagi setiap penggunanya, sebab yang menjadi masalah terkadang bukan berasal dari mesin atau sistemnga melainkan sumber daya manusianya. Teknologi yang semakin canggih saat ini sangat dapat dimanfaatkan untuk meminimalisir kerugian tersebut, seperti analoginya bahwa juga dapat menghalau orang yang akan merugikan kita dengan salah satu caranya ialah mengunci pintu agar penyusup tidak dapat masuk.

Berbagai hal dapat dilakukan oleh penyusup untuk membobol sistem keamanan jaringan komputer melalui penghancuran informasi, pencurian informasi bahkan peretasan software dan hardware. Pencurian yang dimaksud disini tidak hanya mengambil hak yang bukan milik tetapi juga tindakan penyusup untuk menyebarkan informasi pihak tertentu yang sebenarnya tidak memiliki akses pada informasi tersebut. Berikut ini beberapa ancaman yang dapat terjadi pada sistem keamanan jaringan komputer:(Albar & Putra, 2022)

- Denial Of Service (Dos/DDos)

  Ini merupakan ancaman yang disengaja agar dapat menghalangi akses pengguna legalnya. Serangan ini dilakukan dengan menjadi server down sebab adanya permintaan pelayanan yang dilakukan secara konsisten pada skala yang besar, sehingga server tidak dapat memberikan layanan sebab alamat IP melakukan flood ke server secara konsisten.

- SQL Injection

  Contoh ancaman ini pada sebuah perusahaan dengan database yang menyimpan seluruh data digital perusahaan penyerang memanfaatkan hal ini dengan melemahkan SQL server.

- Trojan Horse

  Ancaman ini terlihat seperti program biasa yang memperlihatkan adanya aktivasi yang berguna namun ternyata program tersebut secara sembunyi-sembunyi melakukan

penghapusan data pengguna. Serangan ini dilakukan dengan cara tertutup dan dikemas dengan instruksi yang tidak mencurigakan yang dapat digunakan pada instruksi saat suatu program ditulis.

- Virus

  Virus dikenal sebagai ancaman pada sistem keamanan jaringan komputer yang beroperasi pada platform hardware tertenty dengan desain yang dirancang untuk melemahkan sistem tersebut. Virus dilakukan melalui sejumlah instruksi yang dapat dieksekusi dengan menularkan pada program lainnya dengan adanya modifikasi program yang terinfeksi oleh virus tersebut.

- Bacterium

  Ialan suatu ancaman yang digunakan untuk menggandakan dirinya sehingga dapat merugikan sumber daya yang ada yang berkembang dalam satu mesin.

- Worm

  Ancaman worm memiliki kesamaan dengan ancaman bacterium dimana worm merupakan proses penggandaan diri untuk dapat menginstal duplikat yang digunakan pada mesin dengan jaringan.

- Trap door

  Ancaman ini berupa titik-tik yang dapat masuk tanpa adanya jejak sehingga dapat memberikan akses tanpa adanya proses autentikasi yang seharusnya.

- Logic Bomb

  Merupakan suatu Logika yang menempel pada sistem program komputer dengan tujuan agar pemeriksaan kondisi pada sistem. Sehingga apabila kondisi tersebut teridentifikasi maka Logika akan menjalankan fungsinya agar aktivitas tidak diotorisasi.

3. METODE PENELITIAN

Aktivitas penelitian ini menggunakan jenis penelitian kualitatif deskriptif dengan menggunakan metode studi pustaka. Metode studi pustaka ialah suatu pengumpulan data yang dilakukan melalui aktivitas membaca dan mencatat hal-hal yang berkenaan dengan topik pembahasan melalui dokumen, jurnal atau penelitian terdahulu yang telah dilakukan. Aktivitas penelitian ini dimulai dengan mencari sumber terpercaya, mencatat semua informasi dan menuangkan dalam bentuk tulisan. Penulis melakukan aktivasi analisis penggunaan metode port knocking untuk meningkatkan sistem keamanan jaringan komputer melalui penelitian terdahulu dan data-data yang selanjutnya menyimpulkan hasil dari penelitian apakah dapat meningkatkan sistem keamanan jaringan komputer melalui penggunaan metode port knocking.

4. HASIL DAN PEMBAHASAN

Konsep dan Mekanisme Port Knocking dalam 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 (Riska et al., 2018). 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. 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 (Firdaus dan Fitriawan, 2018)

Pengaplikasian metode Port Knocking pada sistem kemanan yang ada dalam jaringan komputer dapat memberikan sinyal untuk sistem agar menolak adanya proses login apabila sistem tersebut salah atau tidak memberikan parameter tambahan. Dilain sisi admin jaringan juga akan mendapatkan informasi bahwasanya ada aktivitas di sistem jaringan yang berasal dari luar dan gagal dalam melakukan pengakses sistem dengan port yang ada, sehingga sistem dapat melakukan kebutuhan keamanan bagi jaringan komputer, 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 jaringan server. 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 (Albar & Putra, 2022).

Implementasi Port Knocking pada Router Mikrotik dan Studi Kasus

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 (Riska et al., 2018). 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 (Langoben, Rachmawati, 2019)

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 computer (Dwi dan Prakoso, 2022). 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.

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.

5. KESIMPULAN DAN SARAN

Berdasarkan temuan penelitian, Port Knocking merupakan salah satu metode keamanan jaringan yang efektif dalam menyembunyikan port dari akses luar dan hanya mengizinkan akses berdasarkan pola tertentu yang telah ditentukan. Implementasinya pada perangkat seperti router Mikrotik terbukti mampu meningkatkan perlindungan terhadap ancaman seperti brute force dan akses tidak sah, terutama pada jaringan dengan aktivitas tinggi. Metode port knocking dapat meningkatkan sistem keamanan jaringan komputer melalui cara kerja yang dapat

menutup seluruh port, namun user tetap dapat memanfaatkan dan mengakses sistem melalui knocking untuk membuka port yang diizinkan, sehingga sistem kemanan jaringan komputer dapat meningkatkan untuk menghindari ancaman-ancaman.

Penggunaan Port Knocking perlu diimbangi dengan pengaturan firewall yang fleksibel dan pelatihan bagi administrator jaringan agar dapat mengelola sistem secara optimal. Untuk penelitian selanjutnya, disarankan agar dilakukan pengujian pada skala jaringan yang lebih besar atau multi-site, serta mengombinasikan Port Knocking dengan metode keamanan lain seperti VPN dan IDS/IPS untuk meningkatkan efektivitas perlindungan dan meminimalisasi potensi celah keamanan yang masih mungkin terjadi.

DAFTAR REFERENSI

Albar, R., & Putra, R. O. (n.d.). *Menggunakan metode port knocking network security analysis using the method sniffing and implementation of network security on MikroTik Router OS v6.48.3 using port knocking method*. *Journal of Informatics and Computer Science, 8*(1).

Dwi, R., & Prakoso, Y. (2022). Implementasi low interaction honeypot and port knocking untuk meningkatkan keamanan jaringan. *Jurnal Teknologi Informasi dan Komputer, 2*(1), 16–23.

Firdaus, & Fitrawan. (2018). Implementasi keamanan MikroTik menggunakan metode simple port knocking pada SMAN 1 Ngantang. *Jurnal Teknologi Informasi*, *9*(1), 133–140.

Jamalul'ain, A., & Nurdiawan, O. (n.d.). Optimalisasi keamanan jaringan komputer menggunakan metode knocking port berbasis MikroTik (Studi kasus: CV. Mitra Indexindo Pratama). *Jurnal Mahasiswa Teknik Informatika, 6*(2). https://doi.org/10.36040/jati.v6i2.5285

Kusuma, A. P. A. (n.d.). Implementasi simple port knocking pada dynamic routing (OSPF) menggunakan simulasi GNS3. *Jurnal Manajemen Informatika, 5*(2), 7–17.

Langobelen, R., & Rachmawati, D. I. (2019). Analisis dan optimasi dari simulasi keamanan jaringan menggunakan firewall MikroTik (Studi kasus di Taman Pintar Yogyakarta). *JARKOM, 7*(2), 95–102.

Mardiansyah, A. Z., Abdussyakur, Y. M., & Jatmika, A. H. (n.d.). Optimasi port knocking dan honeypot menggunakan IPTables sebagai keamanan jaringan pada server. *Jurnal Teknologi Informasi dan Komputer, 3*(2). https://doi.org/10.29303/jtika.v3i2.144

Mulyanto, K. Y. (n.d.). Analisis dan pengembangan infrastruktur jaringan komputer dalam mendukung implementasi sekolah digital. *JINTEKS, 1*(1), 58–67.

Novianto, D., Tommy, L., & Setiawan Japriadi, Y. (n.d.). Implementation of a network security system using the simple port knocking method on a MikroTik-based router. *JURNAL KOMITEK, 1*(2), 407–417.

Nurnaningsih, R., & Anniar, H. (n.d.). Analisis keamanan jaringan hotspot dengan parameter Quality of Service (QoS) pada Kantor Dinas Komunikasi dan Informatika Kabupaten Soppeng. *JISTI, 5*(1). https://doi.org/10.57093/jisti.v5i1.109

Oktaviansyah, P. D. (n.d.). Penerapan sistem pengamanan port pada MikroTik menggunakan metode port knocking. *Journal of Network and Computer Applications, 1*(2), 13–24.

Riska, P., Sugiartawan, P., & Wiratama, I. (n.d.). Sistem keamanan jaringan komputer dan data dengan menggunakan metode port knocking. *Jurnal Sistem Informasi dan Komputer Terapan Indonesia, 1*(2), 53–64. https://doi.org/10.33173/jsikti.12

Santoso, N. A., Affandi, K. B., & Kurniawan, R. D. (n.d.). Implementasi keamanan jaringan menggunakan port knocking. *Jurnal Janitra Informatika dan Sistem Informasi, 2*(2), 90–95. https://doi.org/10.25008/janitra.v2i2.156

Saputro, A., Saputro, N., & Wijayanto, H. (n.d.). Metode demilitarized zone dan port knocking untuk keamanan jaringan komputer. *Cyber Security, 3*(2). https://doi.org/10.14421/Csecurity.2020.3.2.2150

Saputro, A., Saputro, N., Wijayanto, H., & Informatika, P. S. (n.d.). Metode demilitarized zone dan port knocking untuk keamanan jaringan komputer. *Metode, 3*(2), 22–27.

Suryono, D., & Chandra, D. W. (n.d.). Analisis keamanan jaringan hardware trojan pada IoT. *Jurnal Teknik Informatika dan Sistem Informasi, 9*(4). https://doi.org/10.35957/jatisi.v9i4.2845

Syahputra, H. S., & Wijaya, R. (n.d.). Pembangunan jaringan hotspot berbasis MikroTik pada Kampung Tematik di Kecamatan Padang Utara. *Majalah Ilmiah UPI YPTK*, 29(1), 60–66. https://doi.org/10.35134/jmi.v29i1.108

Yudi Mulyanto, M. J., & Afahar, A. J. (n.d.). Implementasi port knocking untuk keamanan jaringan SMKN 1 Sumbawa Besar. *JINTEKS (Jurnal Informatika Teknologi dan Sains), 3*(2), 326–335.