**Jurnal Sistim Informasi dan Teknologi**

https://jsisfotek.org/index.php

2023 Vol. 5 No. 1 Hal: 102-108 e-ISSN: 2686-3154

# Analisis Penggunaan Metode Port Knocking pada Sistem Keamanan Jaringan Komputer (Studi Kasus di Universitas Baiturrahmah)

Roby Nurbahri, Yuhandri, Gunadi Widi Nurcahyo
Universitas Putra Indonesia YPTK Padang

nurbahriroby@gmail.com

**Abstrak**

Sistem keamanan jaringan digunakan untuk mencegah dan mengidentifikasi masuk pengguna yang tidak sah (penyusup) di jaringan komputer. Tujuannya adalah untuk mengantisipasi bahaya jaringan komputer, yang berupa ancaman fisik atau logik. Ancaman fisik adalah ancaman yang merusak komponen fisik atau perangkat keras komputer, sedangkan ancaman logik meliputi pencurian data atau peretasan akun. Pihak-pihak yang tidak dapat dipercaya dapat menyalahgunakan akses ke sistem keamanan yang tidak dieksploitasi secara maksimal dan menimbulkan risiko yang signifikan. Serangan terhadap keamanan jaringan dilakukan dengan terlebih dahulu mempelajari detail port yang terbuka, kemudian memanfaatkannya. Mayoritas cracker menggunakan sistem port terbuka untuk menyerang sistem jaringan. sebagai ilustrasi, Serangan Dos atau ddos yang menargetkan host atau komputer target dengan sejumlah besar paket yang datang dari beragam host.. Dalam hal ini cracker perlu mengetahui port yang terbuka dan target agar serangan ini berhasil. Serangan masuk lewat celah terbuka di jaringan komputer, salah satunya adalah port yang terbuka, sehingga memungkinkan pengguna internet yang tidak memiliki izin akses atau yang tidak berkepentingan dapat dengan mudah mengelola port-port yang terbukaIde di balik metode port-knocking adalah menyembunyikan layanan jarak jauh di balik Firewall dan hanya mengizinkan akses ke port tersebut ketika klien dapat diautentikasi ke firewall. Hal ini dapat bertindak sebagai pencegah serangan zero-day dan membantu mencegah pemindai menemukan service yang tersedia dan dapat diakses pada host. Dalam hal ini blocking port dapat melindungi firewall dari pemindai.

**Kata kunci**: Keamanan, Jaringan, Metode Port Knocking.

*JSISFOTEK is licensed under a Creative Commons 4.0 International License.*

## 1. Pendahuluan

Jaringan Komputer adalah sekelompok komputer otonom yang saling berhubungan antara satu dengan lainnya menggunakan protokol komunikasi melalui media komunikasi sehingga dapat saling berbagi informasi, program-program, penggunaan bersama perangkat keras seperti printer, harddisk, dan sebagainya. Suatu jaringan komputer terdiri dari komputer, software, dan perangkat jaringan yang bekerja bersama dalam satu ruang lingkup yang disebut jaringan [1]. perkembangan Teknologi Informasi (TI) sangat pesat, dibuktikan dengan semakin canggihnya dunia Teknologi Informasi dariwaktu ke waktu. Dengan semakin canggihnya Teknologi Informasi saat ini memberikan kemudahan pada manusia dalam berkomunikasi [2]. TCP/IP (Transmission Control Protocol/Internet Protocol) digunakan sebagai standar komunikasi data yang digunakan pengguna internet untuk bertukar data antar komputer dalam jaringan internet.. Protokol ini merupakan bagian dari rangkaian (protocol suite) sehingga tidak dapat berdiri sendiri. protokol jenis tersebut saat ini menjadi protokol dengan jumlah terbanyak penggunanya . [3] Untuk melayani miliaran pengguna di seluruh dunia, Internet (jaringan yang saling terhubung) menggunakan sistem protokol kontrol transmisi standar global / rangkaian protokol Internet (TCP / IP) untuk pertukaran paket [4]. Port dalam protokol TCP atau UDP, sebuah komponen dari lapisan Transport OSI, adalah port yang digunakan untuk komunikasi. [5]

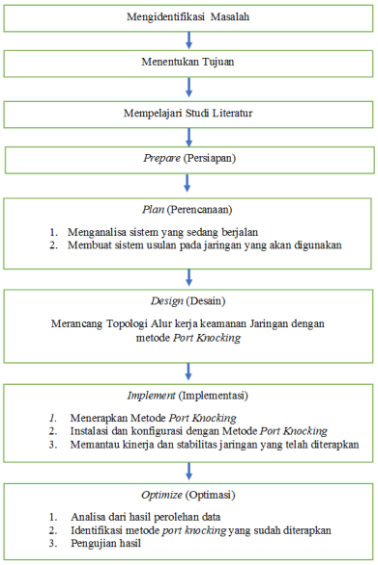
Keamanan jaringan menjadi penting dan harus selalu jadi perhatian, baik Local Area Network (LAN) maupun jaringan Nirkabel atau wireless yang terhubung ke internet pada dasarnya tidak aman dan selalu rentan terhadap peretasan. Karena data harus melewati beberapa terminal untuk mencapai tujuannya, hal ini menciptakan kemungkinan bagi pengguna lain yang tidak bertanggung jawab untuk mengubah, mengganti, merusak, atau bahkan mencuri data (Attacker). [6] Salah satu komponen jaringan paling penting adalah keamanan jaringan. Namun, masalah keamanan jaringan sering kali kurang diperhatikan. Untuk meningkatkan keamanan jaringan, administrator hanya berusaha menggunakan pertahanan terbaik sejauh ini, seperti firewall dan sistem deteksi intrusi (IDS) [7], [8]. 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 [9]. 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. Adapun tahapan yang dilakukan penyerang dalam melakukan penyerangan ialah melakukan identifikasi komputer target atau tahap *port scanning*, penyerang dapat mengambil informasi *port-port* yang terbuka pada mesin target [10]. Serangan *Distributed Denial of Services* (DDoS)

Diterima: xx-xx-20xx | Revisi: xx-xx-20xx | Diterbitkan: xx-xx-20xx | doi: 10.37034/jsisfotek.v5i1.211

mempengaruhi korban dalam bentuk menemukan bug atau kelemahan untuk mengganggu layanan atau menghabiskan semua bandwidth sumber daya dari sistem korban[11]. Metode untuk menemukan port yang terbuka pada komputer adalah pemindaian port atau port scanning. Pada komputer lain yang terhubung ke jaringan, kita dapat melakukan pemindaian port dengan tujuan adalah untuk melihat beberapa port yang terbuka pada komputer [12].
Suatu mekanisme autentikasi pada server yang hanya diketahui oleh user yang menggunakannya disebut port knocking. Manfaat menggunakan port knocking ini dapat menutup semua port jaringan, mencegah penyerang menemukan port yang terbuka jika pemindaian dilakukan. Namun, klien harus mengetuk dengan tepat untuk membuka port yang tertutup [13] Untuk melindungi server dari pemindaian port dan serangan scripts kiddies, dilakukan dengan metode Port Knocking guna mencegah port agar tidak terbuka sambil memungkinkan akses jarak jauh. Setelah memberikan akses user ke port, pengguna kemudian harus menutup port sehingga firewall dapat menghapus rule yang sebelumnya ditulis dalam pembukaan port [14]. Ketika seseorang menggunakan port knocking, port ditutup dan hanya beberapa pengguna tertentu yang diizinkan mengakses. Sementara itu, firewall menutup semua port, terlepas dari user yang memiliki hak akses untuk menggunakannya.[15] [16].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[17].
Pengguna dapat mengubah perangkat berbasis PC menjadi perangkat lunak router menggunakan MikroTik RouterOS, sebuah sistem operasi berbasis Linux. Beberapa fitur-fitur MikroTik RouterOS yakni routing protocol , bandwidth management, firewall rule, dan VPN Server.*[18]. MikroTik Cloud Router Switch* (CRS) merupakan sebuah perangkat Switch yang menggunakan sistem operasi RouterOS MikroTik di dalamnya dan mampu melakukan manajemen *traffic* layer 3 (Routing). Biasanya MikroTik CRS ini dikenal dengan switch Layer3. Secara kinerja MikroTik CRS juga menjalankan RouterOS, yang mana semua fungsi RouterOS dapat diakses oleh perangkat ini. Secara keseluruhan, MikroTik CRS menjalankan peran sebagai switch di Distribution Layer. [19]. Kemampuan untuk mempelajari paket data secara real time dengan Wireshark sangat membantu. Dengan kata lain, melalui antarmuka yang ditentukan pengguna, aplikasi wireshark ini akan melacak semua paket data yang masuk dan keluar. Fakta bahwa Wireshark dapat menganalisis paket data secara real time berarti bahwa Wireshark secara aktif memantau semua paket data yang masuk dan keluar saat berjalan [20].

## 2. Metode Penelitian

Metodologi penelitian adalah sistematika kegiatan penelitian dalam bentuk rancangan untuk menyusun segala hal dalam bentuk proses guna memudahkan dalam hal analisis data, penentuan hasil pembahasan serta kesimpulan dari penelitian.. Berikut ini kerangka atau rancangan kerja dari penelitian yang tersaji pada Gambar 1:



Gambar 1 Kerangka Kerja Penelitian

Pada Gambar 1 dijelaskan kerangka kerja menggunakan metode *Port Knocking* yang mana penjelasannya sebagai berikut:

1. Mengidentifikasi Masalah
   Langkah pertama dalam penelitian ini adalah mengidentifikasi masalah. Peneliti merumuskan suatu masalah atau persoalan kemudian mengerucutkan menjadi subjek atau parameter yang relevan sebagai objek penelitian.
2. Menentukan Tujuan
   Tujuan penelitian perlu dirumuskan untuk memastikan bahwa peneliti tetap berada di jalur yang tepat untuk mencapai hasil yang diinginkan. Batasan dan ruang lingkup masalah dijelaskan pada tahap ini.
3. **Mempelajari Studi Literatur**
   Untuk memiliki landasan teori yang kuat yang akurat dan dijelaskan oleh para peneliti dan profesional terdahulu, membaca literatur menjadi tahap terpenting juga.
4. *Prepare* (Persiapan)
   Tahap persiapan ini peneliti menyusun beberapa perangkat keras dan perangkat lunak yang diperlukan sesuai penggunaan metode Port Knocking dalam implementasi keamanan pada jaringan.

Adapun Perangkat yang disiapkan tertera pada tabel 1 berikut :

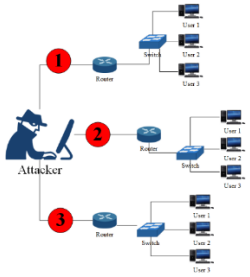
Tabel 1. Kebutuhan Perangkat Keras

| No. | Perangkat Keras | Keterangan |
|---|---|---|
| 1. | Router Mikrotik Routerboard CCR1009-7G-1C-1S+ | Router Mikrotik Sebagai media penghubung dan pemantau lalulintas jaringan |
| 2. | Kabel UTP Category 6 | Media penghubung |
| 3. | Server | Windows dan Linux |

5. *Plan* (Perencanaan)
   Pada tahap perencanaan, peneliti memeriksa sistem yang ada dan mengembangkan sistem yang disarankan untuk jaringan yang digunakan. Analisis ini digunakan sebagai panduan saat mendesain jaringan untuk metode Port Knocking.
6. *Design* (Desain)
   Dalam hal ini peneliti membangun topologi jaringan dengan menggunakan Cisco Packet Tracer - Networking Simulation Tool dan Microsoft Visio untuk menjelaskan gambaran alur kerja dari keamanan jaringan Port Knocking yang akan digunakan.
7. *Implement* (Implementasi)
   Tahapan ini peneliti menerapkan sistem perencanaan berdasarkan pada tahapan sebelumnya melalui simulasi berbasis router Mikrotik dengan seri Routerboard CCR1009-7G-1C-1S+ router ini memiliki spesifikasi dengan CPU TLR4-00980CH-10CE-A3 1.2 GHz 9 Cores, RAM 2 GB Onboard, main storage/NAND 128MB, SFP Port 2, LAN Port 7, RouterOS License Level 6, POE Input 14-57VDC, Memory Card Type MicroSD dan sudah dilengkapi dengan Current Monitor. Tujuannya untuk mendapatkan hasil maksimal ketika diterapkan langsung menggunakan alat-alat yang asli pada sistem berjalan.
8. *Optimize* (Optimasi)
   Peneliti mempelajari hasil analisis data pada tahap ini dengan tujuan untuk menentukan sistem yang diimplementasikan telah berfungsi dengan optimal atau masih memerlukan perbaikan dalam upaya meningkatkan keamanan jaringan yang diterapkan.
9. Pengujian Hasil
   Pengujian diperlukan pada saat ini untuk memastikan hasil dari konfigurasi yang dibuat. Pengujian dilakukan dengan percobaan mengakses router sebelum dan sesudah menggunakan teknik port knocking, serta sniffing, yang melibatkan scanning pada port yang rentan attacker.

## 3. Hasil dan Pembahasan

Perancangan simulasi serangan sniffing dan ddos terhadap jaringan dimulai dengan observasi jaringan router sebelum dilakukan serangan,




Gambar 2 Tahapan Pengujian

Tahapan Pengujian serangan pada gambar 2 di atas adalah sebagai Berikut :
1. Pengujian ketika jaringan Normal (keadaan seperti yang sudah ada) tanpa penggunaan Port Knocking.
2. Pengujian dilakukan dalam keadaan jaringan telah menggunakan Port Knocking (Aktif)
3. Pengujian Port Knocking pada keadaan (Non Aktif).

Tujuan dari pengujian tiga tahap yang dijelaskan di atas adalah untuk menentukan tingkat keamanan jaringan saat ini yang masih bisa dieksploitasi oleh Attacker, dan tujuan kedua adalah untuk menentukan apakah konfigurasi bawaan untuk implementasi port knocking berhasil dan berfungsi sebagaimana mestinya atau tidak.

Jenis serangan yang dikenal sebagai packet sniffing bekerja mengumpulkan data dari paket-paket yang bergerak melalui jaringan. Beberapa data Informasi yang bergerak melalui jaringan dapat berupa nama pengguna, kata sandi, dan data penting lainnya. Pengujian serangan sniffing digunakan untuk menilai tingkat keamanan jaringan dan menggunakan sejumlah komponen yang sudah tersedia.

Tabel 2 Scaning Port

| No. | Port | Service | Status |
|---|---|---|---|

| | | | |
|---|---|---|---|
| 1 | 21 | FTP | Open |
| 2 | 23 | Telnet | Open |
| 3 | 53 | Domain | Open |
| 4 | 80 | http | Open |
| 5 | 8291 | Winbox | Open |

Pada Tabel 2 menunjukkan hasil pengujian serangan *port scanning* yang bertujuan menemukan berbagai informasi *port* yang terbuka dilakukan *attacker sniffing.*

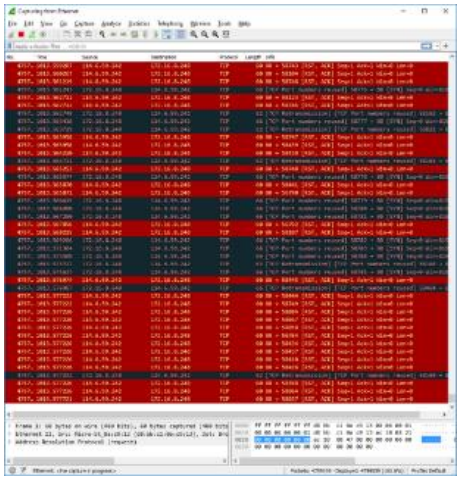
Serangan DDoS beroperasi melalui proses sederhana, dengan tujuan utama untuk membebani server, layanan, atau jaringan dengan traffic yang melewati kapasitas. Hanya dengan satu sistem komputer dapat melakukan serangan ini. Selain situs web, peretas juga menargetkan layanan atau program online, menjadikannya offline atau down sehingga sulit diakses pengguna.

Tabel 3 Serangan DoS

| No. | Host | Tujuan | Protokol | Port |
|---|---|---|---|---|
| 1 | 172.16.8.2 | 114.6.59.242 | ICMP | 1 |
| 2 | 172.16.8.3 | 114.6.59.242 | ICMP | 1 |
| 3 | 172.16.8.4 | 114.6.59.242 | ICMP | 1 |
| 4 | 172.16.8.5 | 114.6.59.242 | ICMP | 1 |
| 5 | 172.16.8.6 | 114.6.59.242 | ICMP | 1 |
| 6 | 172.16.8.7 | 114.6.59.242 | ICMP | 1 |
| 7 | 172.16.8.8 | 114.6.59.242 | ICMP | 1 |
| 8 | 172.16.8.9 | 114.6.59.242 | ICMP | 1 |
| 9 | 172.16.8.10 | 114.6.59.242 | ICMP | 1 |
| 10 | 172.16.8.11 | 114.6.59.242 | ICMP | 1 |

Tabel 3 menunjukkan bahwa serangan DDoS dimulai oleh peretas dengan mengendalikan sejumlah komputer host. Peretas membutuhkan sejumlah besar komputer guna dapat membanjiri server situs web target dengan traffic melebihi batas.

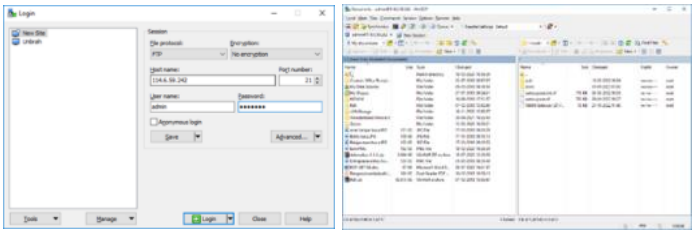
Pada penggunaan DNS Flood Master (Hping3) untuk mensimulasikan serangan DoS pada router dianalisis apakah serangan DoS yang dilancarkan telah efektif menembus jaringan router. Dalam skenario tersebut, digunakan aplikasi Wireshark untuk menganalisis serangan DoS pada router sekaligus melihat kemampuan aplikasi tersebut mengenal dan mendeteksi serangan pada router.



Gambar 3. Trafik Ping Pada Wireshark Saat Serangan

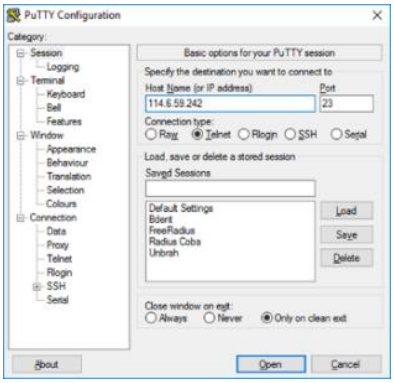
Gambar 3 menunjukkan terjadinya serangan DoS yang dilakukan penyerang melalui proses pengiriman Ping ke target jaringan router.

Pada pengujian berikutnya dilakukan sniffing yang ditujukan pada protocol FTP (21) target melakukan login via FTP dengan memanfaatkan aplikasi WinSCP. Proses login via FTP dan lalu lintas data yang nantinya akan direkam dan dianalisis oleh wireshark untuk mendapatkan informasi apa saja yg diinputkan oleh host,dapat dilihat pada gambar 4.



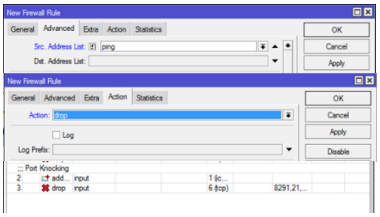
Gambar 4. FTP Login

Tahapan selanjutnya melakukan simulasi serangan Sniffing Attack pada protocol Telnet (23) menggunakan wireshark untuk mengukur tingkat intensitas serangan Sniffing Attack yang diluncurkan dalam menembus jaringan router.



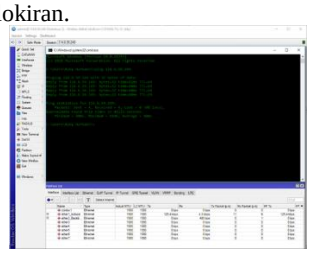

Gambar 5. Login Telnet

Port knocking merupakan sebuah teknik yang mana memungkinkan perangkat jaringan untuk mendapatkan akses ke beberapa port yang telah dibatasi oleh firewall dengan mengirimkan paket atau koneksi tertentu seperti TCP, UDP, dan ICMP. Dalam prosesnya firewall secara dinamis akan memberikan akses ke port yang diblok jika koneksi yang dikirim oleh host sesuai dengan rule knocking yang digunakan.




Gambar 6. Advanced Firewall Rule

Gambar 6 menunjukkan informasi trafik selain IP yang telah terdaftar dengan menggunakan logika NOT (!) . Langkah selanjutnya adalah menggunakan action = drop dan seluruh rule Firewall Filter yang telah dikonfigurasi dalam Firewall rule untuk menentukan tindakan pada alasan pemblokiran.



Gambar 7. Login via Winbox

Gambar 7 menunjukkan pengujian yang dapat dilakukan dengan menghubungkan winbox ke router tanpa melakukan ping terlebih dahulu; dalam kasus ini, akses akan ditolak, tetapi menghubungkan winbox ke router setelah melakukan ping akan berhasil.

Berdasarkan pengujian port knocking yang dilakukan melalui penyerangan sniffer Hal ini dapat meningkatkan keamanan perangkat jaringan seperti router . karena Administrator jaringan dapat melakukan blokir pada port yang rentan pada serangan antara lain Winbox (tcp 8291), SSH (tcp 22), Telnet (tcp 23), dan webfig (tcp 80). Port-port ini akan tampak tertutup ketika dilakukan pemindaian port .Skenario penerapan metode port Knocking pada router mikrotik didapati hasil sesuai bahwa setelah dilakukan serangan dengan sniffing attacker di mana attacker tidak bisa mendeteksi dan mengakses port yang sudah diterapkan *Port Knocking* pada konfigurasinya.

## 4. Kesimpulan

Pengujian sistem keamanan jaringan dengan metode Port Knocking untuk mengamankan Router dapat diterapkan pada router Mikrotik dengan pemanfaatan firewall yang berfungsi untuk menjaga akses ilegal dan mengatasi permasalahan yang disebabkan oleh Attacker.

## Daftar Rujukan


[1] Saputro, A., Saputro, N., & Wijayanto, H. (2020). *Metode Demilitarized Zone Dan Port Knocking Untuk Keamanan Jaringan Komputer* (Vol. 3, Issue 2). Https://Doi.Org/10.14421/Csecurity.2020.3.2.2150

[2] Jamalul'ain, A., & Nurdiawan, O. (2022). Optimalisasi Keamanan Jaringan Komputer Menggunakan Metode Knocking Port Berbasis Mikrotik (Studi Kasus: CV. Mitra Indexindo Pratama). In *Jurnal Mahasiswa Teknik Informatika)* (Vol. 6, Issue 2). https://doi.org/10.36040/jati.v6i2.5285

[3] Mardiansyah, A. Z., Abdussyakur, Y. M., & Jatmika, A. H. (2021). *Optimasi Port Knocking Dan Honeypot Menggunakan Iptables Sebagai Keamanan Jaringan Pada Server (Port Knocking and Honeypot Optimization using IPTables for Serverrs Network Security )*. https://doi.org/10.29303/jtika.v3i2.144

[4] Syahputra, H. S., & WIjaya, R. (2022). Pembangunan Jaringan Hotspot Berbasis Mikrotik pada Kampung Tematik di Kecamatan Padang Utara. *Majalah Ilmiah UPI YPTK*, 60–66. https://doi.org/10.35134/jmi.v29i1.108

[5] al Amien, J. (2020). *Implementasi Keamanan Jaringan Dengan Iptables Sebagai Firewall Menggunakan Metode Port Knocking*. https://doi.org/10.37859/jf.v10i2.2098

[6] Albar, R., & Putra, R. O. (2022). Menggunakan Metode Port Knocking Network Security Analysis Using The Method Sniffing And Implementation Of Network Security On Microtik Router Os V6.48.3 Using Port Knocking Method. *Journal of Informatics and Computer Science*, *8*(1). https://doi.org/10.33143/jics.Vol8.Iss1.1997

[7] Wiryadinata, R. (2022). Rancang Bangun Keamanan Port Secure Shell (SSH) Menggunakan Metode Port Knockking. In *Sains Teknik Elektro* (Vol. 3, Issue 1). https://doi.org/10.31294/instk.v3i1.552

[8] Suryono, D., & Chandra, D. W. (2022). Analisis Keamanan Jaringan Hardware Trojan Pada IoT. *Jurnal Teknik Informatika Dan Sistem Informasi*, *9*(4). https://doi.org/10.35957/jatisi.v9i4.2845

[9] Nurnaningsih, Riskayani, & Husnang Anniar. (2022). Analisis Keamanan Jaringan Hotspotdengan Parameter Quality Of Service (Qos) Pada Kantor Dinas Komunikasi Dan Informatika Kabupaten Soppeng. In *Jisti* (Vol. 5, Issue 1). https://doi.org/10.57093/jisti.v5i1.109

[10] Novianto, D., Tommy, L., & Setiawan Japriadi, Y. (2021). 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. *JURNAL KOMITEK*, *1*(2), 407–417. https://doi.org/10.53697/jkomitek.v1i2

[11] Saputro Andik, Tunggono Saputro Daniel, & Remawat Dwi. (2022). *Implementasi Port KnockingUntuk Keamanan Jaringan Komputer Dengan Metode Demilitarized Zone*. https://doi.org/10.46808/informa.v8i2.222

[12] Pratama, R., & Wijaya, A. (2022). Strategi Pengamanan Akses Jaringan Dengan L2TP Over IP Security Pre-shared Key Dan Port Knocking. In *Jurnal JUPITER* (Vol. 14, Issue 2). Bulan Oktober. Https://Doi.Org/10.5281./5096/5.Jupiter.2022.10

[13] Zainal Amir Mahmud, M., & Risqiwati, D. (2020). Implementasi Asymmetric Encryption RSA Pada Port Knocking Ubuntu Server Menggunakan Knockd Dan Python. *REPOSITOR*, *2*(6), 787–794. https://doi.org/10.22219/repositor.v2i6.270

[14] Dwi, R., & Prakoso, Y. (2022). *Implementasi Low Interaction Honeypot Dan Port Knocking Untuk Meningkatkan Keamanan Jaringan*. https://doi.org/10.54199/pjse.v2i1.96

[15] Ernawati, R., Ruslianto, I., Bahri, S., Rekayasa, J., Komputer, S., Mipa, F., Tanjungpura, U., Prof, J., Hadari, H., & Pontianak, N. (2022). *Implementasi Metode Port Knocking Pada Sistem Keamanan Server Ubuntu Virtual Berbasis Web Monitoring*. Doi: http://dx.doi.org/10.26418/coding.v10i01.54226

[16] Ketut, I., Komang, I., Mogi, A., Rai, C., Santi Astawa, G., Raharja, A., & Agus, N. (2022). *Implementasi Port Knocking Dalam Mengamankan Jaringan VPN Pada Sistem E-Learning*. https://doi.org/10.1155/2022/9153868

[17] Santoso, N. A., Affandi, K. B., & Kurniawan, R. D. (2022). Implementasi Keamanan Jaringan Menggunakan Port Knocking. *Jurnal Janitra Informatika Dan Sistem Informasi*, *2*(2), 90–95. https://doi.org/10.25008/janitra.v2i2.156

[18] Amalia, E. R., Nurheki, Saputra, R., Ramadhana, C., & Yossy, E. H. (2023). Computer network design and implementation using load balancing technique with per connection classifier (PCC) method based on MikroTik router. *Procedia Computer Science*, *216*, 103–111. https://doi.org/10.1016/j.procs.2022.12.116

[19] Jody, M., Walimema, A., & Sulistyo, W. (2023). *Perancangansistemkeamananjaringanberbasishierrchicalnetworkdesign*. https://doi.org/10.35447/jitekh.v10i2.571

[20] Pangestu, T., & Liza, R. (2022). Analisis Keamanan Jaringan pada Jaringan Wireless dari Serangan Man In The Middle Attack DNS Spoofing. *JITEKH*, *10*(2), 60–67. DOI: https://doi.org/10.33365/jsstcs.v3i2.2105