Pukeng, A. F. and Havid, H. (no date) "Security Design for Local Area Networks Using Port Firewall Security", Sebatik, 29(2).
Submitted: 2025-11-22 Accepted: 2025-12-24 Published: 2025-12-26

Sebatik Vol. 29 No. 2 December 2025
ISSN: 1410-3737(p) 2621-069X(e)

DOI:10.46984/sebatik.v29i1.2699

Security Design for Local Area Networks Using Port Firewall Security

Ahmad Fahrijal Pukeng[1)], dan **Hervan Havid**[2]

[1,2]Teknik informatika, STMIK Widya Cipta Dharma
[1,2]Jl. M. Yamin No. 25,Samarinda, 75123
E-mail: pukeng@wicida.ac.id[1)], 2243108@wicida.ac.id[2)]

ABSTRACT

Network security design is a crucial aspect in maintaining data integrity, confidentiality, and availability. This study develops and tests an effective network security system using the firewall security port method. This method focuses on identifying and restricting access to physical switch ports to prevent unauthorized access and protect the system from external threats. The research method uses experimental stages through subjective means to describe current practices. Through configuration and testing in a simulated environment, this study shows that the implementation of MAC address-based port security effectively blocks illegal devices without disrupting the connectivity of legitimate devices. This study provides evidence and practical guidelines that the firewall security port method is an efficient solution for improving network access layer security. The conclusions of this study provide a basis for organizations to implement proactive security measures in the face of evolving cyber threats.

***Keywords**: Firewall, Security, Network, Port Security, MAC Address.*

PERANCANGAN KEAMANAN JARINGAN LOKAL MENGGUNAKAN FIREWALL PORT SECURITY

ABSTRAK

Perancangan keamanan jaringan merupakan aspek krusial dalam menjaga integritas, kerahasiaan, dan ketersediaan data. Penelitian ini mengembangkan dan menguji sistem keamanan jaringan yang efektif menggunakan metode *firewall security* port. Metode ini fokus pada identifikasi dan pembatasan akses ke *port* fisik *switch* untuk mencegah akses tidak sah dan melindungi sistem dari ancaman eksternal. Metode penelitian ini menggunakan tahapan eksperimental melalui cara yang subjektif untuk menggambarkan praktik saat ini. Melalui konfigurasi dan pengujian dalam lingkungan simulasi, penelitian ini menunjukkan bahwa penerapan *port security* berbasis alamat MAC secara efektif memblokir perangkat ilegal tanpa mengganggu konektivitas perangkat yang sah. Penelitian ini memberikan bukti dan pedoman praktis bahwa metode *firewall security port* merupakan solusi efisien untuk meningkatkan keamanan lapisan akses jaringan. Kesimpulan dari penelitian ini menjadi dasar bagi organisasi untuk menerapkan langkah-langkah keamanan proaktif dalam menghadapi ancaman siber yang terus berkembang.

Kata Kunci: Firewall, Keamanan, Jaringan, Port Security, MAC Address.

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi yang pesat telah mendorong transformasi digital di berbagai sektor, yang menuntut adopsi infrastruktur jaringan yang semakin kompleks dan terdistribusi. Seiring dengan tingginya konektivitas, tantangan dalam hal keamanan informasi menjadi semakin signifikan (Melati dkk, 2023). Jaringan komputer yang tidak dilindungi dengan baik berisiko tinggi mengalami berbagai serangan siber, seperti peretasan, pencurian data, penyebaran *malware*, dan serangan *Denial of Service* (DoS), yang dapat merugikan secara finansial maupun reputasi (Ramli, 2023).

Ancaman siber modern terus berevolusi menjadi lebih canggih, menargetkan berbagai lapisan jaringan (Shanker dan Singh, 2021). Oleh karena itu, keamanan jaringan menjadi aspek fundamental untuk menjamin kelangsungan layanan dan melindungi aset digital. Meluasnya penggunaan perangkat *Internet of Things* (IoT) juga memperbesar permukaan serangan (*attack surface*), sehingga menuntut mekanisme pengamanan yang andal dan berlapis (Chen, 2021).

Salah satu pendekatan utama dalam arsitektur keamanan jaringan adalah penggunaan *firewall* sebagai lapisan pertahanan pertama. *Firewall* bekerja sebagai penyaring lalu lintas data antara jaringan internal yang aman dan jaringan eksternal yang tidak dipercaya

(Sharma dkk, 2021). Dalam penelitian ini, fokus utama adalah pada metode *firewall security port*, sebuah teknik pengamanan pada lapisan kedua model OSI (*Data Link Layer*) yang mengendalikan akses terhadap *port* fisik pada perangkat *switch* (Wulan dkk, 2024).

Penerapan *port security* memanfaatkan keunikan alamat fisik perangkat (MAC *address*) (Pratomo, 2023). Dengan konfigurasi yang tepat, *switch* dapat diatur untuk hanya mengizinkan perangkat dengan MAC *address* terdaftar untuk berkomunikasi. *Switch* dapat secara otomatis menonaktifkan *port* jika mendeteksi perangkat tidak dikenal, mencegahnya mengakses jaringan meskipun menggunakan alamat IP yang sah (Dasmen dkk, 2022). Strategi ini memberikan lapisan keamanan tambahan yang efektif untuk mencegah serangan fisik seperti penyisipan perangkat ilegal (*rogue devices*), terutama dalam jaringan skala kecil hingga menengah (Dewi dkk, 2022).

Keamanan jaringan merupakan serangkaian praktik untuk melindungi jaringan dan data dari akses atau perusakan yang tidak sah. Tujuannya adalah menjamin tiga pilar utama yang dikenal sebagai CIA Triad: Kerahasiaan (*Confidentiality*), Integritas (*Integrity*), dan Ketersediaan (*Availability*) (Dwinanto dan Setiyani, 2021). Pelanggaran terhadap salah satu pilar ini dapat mengakibatkan kerugian signifikan. Untuk mencapainya, berbagai teknologi diimplementasikan, mulai dari kontrol akses, enkripsi, hingga sistem deteksi intrusi.

Penelitian ini bertujuan untuk merancang, mengimplementasikan, dan menguji sistem keamanan jaringan menggunakan metode *firewall security port* dalam lingkungan simulasi. Diharapkan hasil penelitian ini dapat menjadi referensi praktis bagi organisasi untuk menerapkan sistem keamanan yang lebih ketat namun tetap efisien.

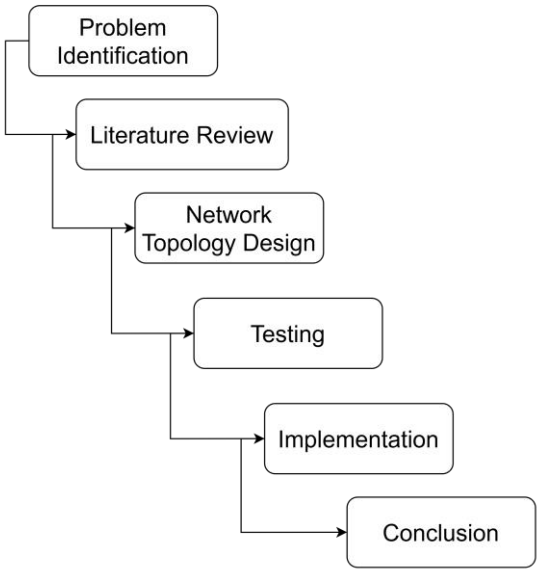
2. RUANG LINGKUP

Ruang lingkup penelitian ini berfokus pada perancangan dan pengujian mekanisme keamanan jaringan pada lapisan akses menggunakan metode *firewall security port* berbasis konfigurasi *port security* pada *switch*.

Permasalahan yang dikaji mencakup pencegahan akses fisik tidak sah ke jaringan lokal, penguncian *port* berdasarkan MAC *address*, serta evaluasi efektivitas konfigurasi ini dalam skenario normal maupun skenario serangan pada lingkungan simulasi berskala kecil.

3. BAHAN DAN METODE

Metodologi penelitian yang digunakan, sebagaimana diilustrasikan pada Gambar 1, disusun berdasarkan kerangka kerja teoritis yang mencakup disiplin keamanan jaringan, topologi jaringan, serta implementasi metode *firewall port security*. Pemahaman yang komprehensif mengenai konsep-konsep tersebut merupakan fondasi esensial bagi eksperimen yang dilaksanakan.



Gambar 1. Tahapan Penelitian
Figure 1. Methodology Stages

Gambar 1 memaparkan pgamemilihan topologi jaringan yang relevan diidentifikasi sebagai faktor determinan untuk mengoptimalkan efektivitas *firewall port security*. Lebih lanjut, identifikasi potensi kerentanan pada topologi tersebut berkontribusi pada optimalisasi langkah-langkah keamanan dan peningkatan resiliensi sistem terhadap ancaman siber (Santoso dkk, 2022). Fokus sentral penelitian ini terletak pada implementasi, konfigurasi, dan pengujian metode *firewall port security*, di mana pengujian dilakukan melalui beberapa langkah verifikasi dalam lingkungan jaringan yang disimulasikan.

Tahap analisis data meliputi evaluasi terhadap metrik keamanan yang telah ditetapkan dan identifikasi pola serangan. Pada bagian akhir, kesimpulan akan meringkas temuan-temuan signifikan, menyajikan arahan untuk riset di masa mendatang, serta memberikan rekomendasi untuk penyempurnaan implementasi keamanan jaringan (Saputra, 2022).

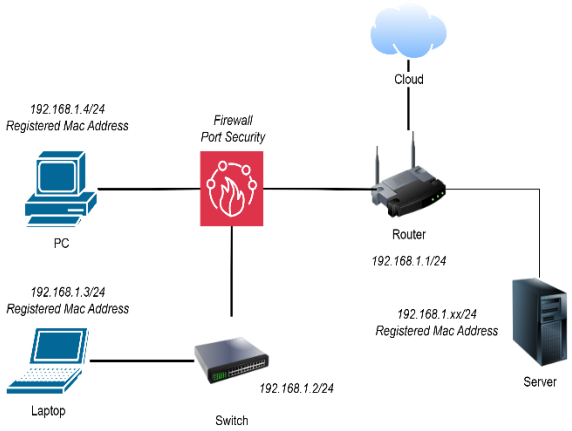
3.1 Bahan dan Perangkat

1. Perangkat Keras (Simulasi) : 1 PC, 1 Laptop, 1 Switch Cisco 2960, dan 1 Router Cisco 1941.
2. Perangkat Lunak : Cisco Packet Tracer versi 8.2 digunakan sebagai platform simulator

3.2 Perancangan Topologi Jaringan

Tahapan inisialisasi dalam perancangan topologi *firewall port security* adalah dengan mengembangkan sebuah arsitektur jaringan yang melibatkan dua *end-point device*, yaitu satu unit PC dan satu unit laptop, seperti yang ditampilkan pada gambar 2. Desain ini dirancang spesifik untuk fortifikasi keamanan pada jaringan berskala terbatas. Dalam arsitektur tersebut, kedua perangkat dihubungkan pada sebuah *hub* sentral, seperti

router atau *switch*, yang kemudian *firewall port security* diinterposisikan di antara hub sentral dan *end-point device* untuk berfungsi sebagai regulator trafik.



Gambar 2. Desain Topologi Jaringan
Figure 2. Network Topology Design

Berdasarkan gambar 2. konfigurasi spesifik, *firewall* akan melakukan filtrasi lalu lintas data dengan memberikan atau menolak akses pada *port-port* tertentu, sehingga hanya trafik yang telah terverifikasi aman yang dapat diteruskan ke perangkat tujuan. Implementasi skema ini menawarkan dua keunggulan utama: memfasilitasi supervisi aktivitas jaringan secara lebih efektif serta menyediakan kontrol yang lebih granular terhadap aksesibilitas *port*.

1. *Firewall* Sebagai Lapisan Pertahanan

Metode *port security* yang dibahas beroperasi pada Layer 2 dan berfungsi sebagai pelengkap *firewall* tradisional, memberikan pertahanan mendalam (*defense-in-depth*) dengan mengamankan titik akses fisik ke jaringan (Putri dkk, 2023; Satria dan Ramadhani, 2023) seperti yang ditampilkan pada tabel 1.

Tabel 1. Perbandingan Jenis-Jenis *Firewall*
Table 1. Comparison of Firewall Types

Firewall Types	OSI Layer	How It Works	Advantages	Disadvantages
Packet Filtering	Network (L3)	Checks packet headers (IP, port) individually	Fast and efficient. Stateless	Vulnerable to IP spoofing
Stateful Inspection	Transport (L4)	Tracks active connection status and makes decisions based on context	More secure, can detect fake packets	Requires more resources
Proxy (Application)	Application (L7)	Acts as an intermediary, deeply inspects payload content	High security at the application level.	Can cause performance bottlenecks
Next-Gen (NGFW)	L3-L7	Combines stateful features, DPI, and integration with other systems (IDS/IPS)	Comprehensive security	Complex and expensive

Sumber: Diadaptasi dari (Wicaksono, 2022)

Tabel 1 menyajikan perbandingan komprehensif antara empat jenis *firewall* yang beroperasi pada lapisan OSI berbeda. *Packet Filtering* merupakan metode paling efisien tetapi rentan terhadap IP *spoofing* karena hanya memeriksa *header* paket pada Layer 3. *Stateful Inspection* meningkatkan keamanan dengan melacak status koneksi aktif pada Layer 4 namun memerlukan sumber daya lebih besar. *Proxy* di Layer 7 menawarkan inspeksi konten yang mendalam dengan keamanan tingkat aplikasi tetapi berpotensi menimbulkan hambatan performa. Sebaliknya, *Next-Gen Firewall* (NGFW) mengintegrasikan semua fitur tersebut untuk memberikan perlindungan komprehensif dari Layer 3 hingga Layer 7, meskipun dengan kompleksitas dan biaya yang lebih tinggi. Dalam konteks penelitian ini, metode *port security* yang diimplementasikan berfungsi sebagai lapisan tambahan yang memperkuat keamanan pada Level 2 (*Data Link Layer*) melalui filtrasi berbasis MAC *address*

2. *Port Security* pada *Switch* Jaringan

Port Security adalah fitur keamanan pada *switch* yang membatasi akses ke antarmuka berdasarkan MAC address perangkat (Nurfaishal dan Akbar, 2024). Fitur ini secara efektif "mengunci" *port* sehingga hanya perangkat terotorisasi yang dapat menggunakannya. Ketika diaktifkan, switch memantau MAC *address* dari *frame* yang masuk.

Ada beberapa mode pelanggaran (*violation mode*) yang dapat dikonfigurasi:

a. *Shutdown*: Mode *default*. *Port* akan segera dinonaktifkan (*err-disabled*) jika terjadi pelanggaran.
b. *Protect*: *Port* membuang paket dari MAC address yang tidak dikenal tanpa notifikasi.
c. *Restrict*: *Port* membuang paket, mencatat pelanggaran, dan mengirim notifikasi SNMP.

Metode *sticky learning* memungkinkan *switch* secara dinamis mempelajari MAC *address* yang terhubung pertama kali dan menyimpannya secara permanen dalam konfigurasi (Novianto dkk, 2023).

3. Skenario Pengujian dan Verifikasi

Dalam proses pengujian dan verifikasi dilakukan 2 skenario yaitu:

1. Skenario Normal: Perangkat sah terhubung, verifikasi dengan *ping* dan *show port-security.*
2. Skenario Serangan: Perangkat ilegal dihubungkan ke *port* yang diamankan, respons *switch* diamati.

4. PEMBAHASAN

Penelitian ini menghasilkan aplikasi jaringan yang dibangun melalui pendekatan keamanan *firewall* dengan metode *port security*. Aplikasi ini mencakup pengaturan jaringan secara fisik (*hardware*), konfigurasi perangkat lunak jaringan (*software*), dan pengamanan logis terhadap akses *port.*

1. Langkah-langkah Konfigurasi dan Implementasi

Langkah-langkah yang perlu dilakukan adalah sebagai berikut:

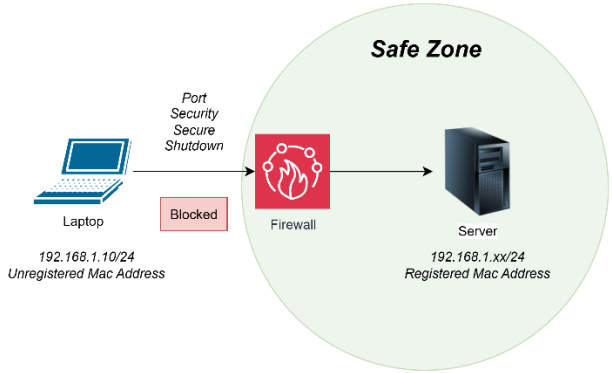
a. Konfigurasi Dasar: Memberikan alamat IP statis pada PC (192.168.1.4/24), Laptop (192.168.1.3/24), *Switch* (192.168.1.2), dan *Router* (192.168.1.1/24).
b. Pengujian Konektivitas Awal: Melakukan uji *ping* antar perangkat untuk memastikan konektivitas dasar.
c. Aktivasi *Port Security*: Mengaktifkan *port security* pada antarmuka *switch* (*FastEthernet0/1* dan *FastEthernet0/2*).
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
d. Konfigurasi Metode MAC Address: Mengatur mode *sticky* dengan batasan 1 MAC address per *port*
S*witch(config-if)# switchport port-security maximum 1*
Switch(config-if)# switchport port-security mac-address sticky
e. Konfigurasi Mode Pelanggaran: Mengatur mode *shutdown*.
Switch(config-if)# switchport port-security violation shutdown

2. Hasil Konfigurasi Awal

Setelah konfigurasi dan menghubungkan perangkat sah, *switch* mempelajari MAC *address* masing-masing dan menguncinya ke *port*. Perintah *show port-security interface Fa0/1* mengkonfirmasi bahwa *port security* aktif, port berstatus *Secure-up*, dan satu *sticky* MAC *address* telah dipelajari, dengan *Security Violation Count* bernilai 0.

3. Hasil Pengujian Skenario Serangan

Pada skenario serangan, "Laptop Peretas" dihubungkan ke *port Fa0/1*. Seketika setelah perangkat ilegal mengirimkan *frame*, switch mendeteksi MAC *address* baru. Sesuai konfigurasi, port Fa0/1 langsung dinonaktifkan. Verifikasi CLI menunjukkan status *port Secure-shutdown* dan *Security Violation Count* meningkat menjadi 1, seperti yang ditampilkan pada gambar 3.



Gambar 3. Ilustrasi Proses Pemblokiran Akses oleh *Port Security*

Figure 3. Illustration of the Access Blocking Process by Port Security

Hasil eksperimen menunjukkan bahwa metode *firewall security port* sangat efektif mencegah akses fisik tidak sah. Mekanisme ini memberikan kontrol granular pada Layer 2 dan hal ini didukung juga dengan penelitian yang dilakukan oleh (Dara dkk, 2022). Keberhasilan *mode shutdown* tidak hanya memblokir penyerang tetapi juga memberi peringatan jelas kepada administrator jaringan seperti yang dilakukan oleh (Firmansyah dk, 2021).

Dibandingkan dengan ACL berbasis IP, *port security* menawarkan keunggulan dalam mengatasi *IP spoofing* karena beroperasi menggunakan MAC *address* yang unik secara fisik. Namun, metode ini memiliki keterbatasan. *Port security* tidak melindungi dari serangan level aplikasi atau serangan dari dalam (*insider threats*). Oleh karena itu, *port security* harus menjadi bagian dari strategi keamanan berlapis (*defense-in-depth*) yang komprehensif, seperti yang ditampilkan pada tabel 2.

Tabel 2. Rangkuman Hasil Pengujian Skenario

Table 2. Summary of Scenario Test Results

Scenario	Action	Expected Result	Actual Result	Status
Normal Connectivity	Valid ping between devices	Connection successful	Connection successful	Successful
Illegal Access Attempt	Illegal device connected	Switch port disabled	Port Fa0/1 Secure-shutdown	Successful
Recovery	Administrator re-enables port	Port functioning again	Port active after no shutdown	Successful

Hasil pengujian pada dua skenario berbeda, sebagaimana dirangkum pada Tabel 2, menunjukkan efektivitas implementasi *port security* dalam sistem keamanan jaringan yang diusulkan. Skenario Normal *Connectivity* mengkonfirmasi bahwa perangkat yang sah (PC dan Laptop dengan MAC *address* terdaftar) dapat berkomunikasi dengan lancar tanpa gangguan, dengan ping antar perangkat berhasil menunjukkan konektivitas penuh. Skenario *Illegal Access Attempt* mensimulasikan ancaman nyata di mana perangkat tidak sah ("Laptop Peretas") mencoba terhubung ke *port* yang telah dikonfigurasi dengan *port security*. Hasil actual yang diperoleh menunjukkan bahwa switch secara otomatis merespons dengan menonaktifkan *port* (*Secure-shutdown*) secepatnya, mencegah penyusup mengakses jaringan internal. Skenario *Recovery* mendemonstrasikan bahwa administrator dapat dengan mudah mengembalikan fungsi *port* melalui perintah CLI tanpa perlu konfigurasi ulang, memastikan fleksibilitas operasional sistem keamanan.

5. KESIMPULAN

Penelitian ini berhasil merancang dan membuktikan bahwa sistem keamanan jaringan menggunakan metode *firewall security port* efektif meningkatkan keamanan pada level akses fisik. Dengan konfigurasi *port security* berbasis MAC *address* dan mode pelanggaran *shutdown*, sistem terbukti mampu mengenali dan memblokir perangkat tidak sah secara otomatis dan seketika. Implementasi ini berhasil menjaga integritas akses jaringan dengan memastikan hanya perangkat terdaftar yang dapat terhubung. Pendekatan ini merupakan solusi keamanan yang praktis, berbiaya rendah, dan efisien untuk organisasi sebagai lapisan pertahanan fundamental.

6. SARAN

Untuk pengembangan lebih lanjut dan penyempurnaan dari sistem yang telah dibangun, berikut adalah beberapa saran yang dapat menjadi acuan bagi penelitian di masa mendatang, yaitu integrasi dengan teknologi lain dengan menggabungkan *port security* dengan *Intrusion Detection System* (IDS) dan *Access Control List* (ACL) untuk menciptakan sistem keamanan yang lebih komprehensif, lalu penerapan pada skala lebih besar dengan menguji implementasi pada topologi jaringan yang lebih kompleks untuk menganalisis tantangan skalabilitas dan manajemen, dan otomatisasi Respons Insiden melalui pengembangan skrip otomatis untuk notifikasi *real-time* kepada administrator saat terjadi pelanggaran

7. REFERENSI

Chen, J., Mohamed, M. A., Dampage, U., Rezaei, M., Salmen, S. H., Obaid, S. A., & Annuk, A. (2021). A multi-layer security scheme for mitigating smart grid vulnerability against faults and cyber-attacks. *Applied Sciences*, *11*(21), 9972.

Dara, Y. C., Hariadi, F., & Lede, P. A. R. L. (2022). Analisis Penerapan Sistem Keamanan Jaringan Menggunakan Metode Dhcp Snooping Dan Switch Port Security. *Jurnal Inovatif*, *1*(3), 187-196.

Dasmen, R. N., Firmansyah, M. H., Khadafi, M., & Yolanda, T. (2022). Penerapan Keamanan Jaringan Menggunakan Metode Firewall Security Port: Network Security Implementation Using Firewall Security Port Method. *Decode: Jurnal Pendidikan Teknologi Informasi*, *2*(1), 1-7.

Dewi, S., Firmansyah, F., & Hasan, U. (2022). Penerapan metode access control list pada jaringan VLAN menggunakan router Cisco. *IMTechno: Journal of Industrial Management and Technology*, *3*(1), 37-41.

Dwinanto, I., & Setiyani, H. (2021). Implementasi Keamanan Komputer Pada Aspek Confidentiality, Integrity, Availability (CIA) Menggunakan Tools Lynis Audit System. *Jurnal Maklumatika*, 35-46.

Firmansyah, F., Purnama, R. A., & Astuti, R. D. (2021). Optimalisasi Keamanan Wireless Menggunakan Filtering MAC Address: Optimalisasi Keamanan Wireless Menggunakan Filtering Mac Address. *Jurnal Teknologi Informasi: Jurnal Keilmuan Dan Aplikasi Bidang Teknik Informatika*, *15*(1), 25-33.

Melati Sukma, W. N., Reynata, A., Yasmine, D. A., & Putra Pratama, D. M. (2023). Systematic Literature Review (SLR): Keamanan Dalam Sistem Informasi. *Journal of Comprehensive Science (JCS)*, *2*(6).

Novianto, E., Ujianto, E. I. H., & Rianto, R. (2023). Keamanan informasi (information security) pada aplikasi sistem informasi manajemen kepegawaian dengan defense in depth. *J-Icon: Jurnal Komputer dan Informatika*, *11*(1), 1-6.

Nurfaishal, M. D., & Akbar, Y. (2024). Analisis Efektivitas Keamanan Jaringan Layer 2: Port Security, VLAN Hopping, DHCP Snooping. *Jurnal Indonesia: Manajemen Informatika dan Komunikasi*, *5*(3), 3278-3290.

Pratomo, A. B. (2023). Pengembangan Sistem Firewall Pada Jaringan Komputer Berbasis Mikrotik Routeros. *Bulletin of Network Engineer and Informatics*, *1*(2), 51-59.

Putri, R. M., Zulkifli, Z., & Fajri, R. M. (2023). *Simulasi Keamanan Jaringan Dengan Metode Network Development Life Cycle Menggunakan Switch Port Security Pada PT Pinus Merah Abadi* (Doctoral dissertation, Universitas indo global mandiri).

Ramli, H., & Alifsyah, M. Y. (2023). Analisis Keamanan Komputer Terhadap Serangan Distributed Denial of Service (DDOS). *J. Renew. Energy Smart Device*, *1*(1), 25-30.

Razzanda, I. M., & Koprawi, M. (2024). Implementasi IDS dan IPS terhadap Serangan TCP Port Scanning dan ICMP Flooding. *The Indonesian Journal of Computer Science*, *13*(4).

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.

Saputra, B. R. (2022). Simulasi Keamanan Jaringan Dengan Metode DHCP Snooping Dan VLAN Mengggunakan CISCO. *JATISI (Jurnal Teknik Informatika dan Sistem Informasi)*, *9*(4), 3481-3488.

Satria, A., & Ramadhani, F. (2023). Analisis Keamanan Jaringan Komputer dengan Menggunakan Switch Port Security di Cisco Packet Tracer. *sudo Jurnal Teknik Informatika*, *2*(2), 52-60.

Shanker, R., & Singh, A. (2021, December). Analysis of Network Attacks at Data Link Layer and its Mitigation. In *2021 International Conference on Computing Sciences (ICCS)* (pp. 274-279). IEEE.

Sharma, G., Vidalis, S., Anand, N., Menon, C., & Kumar, S. (2021). A survey on layer-wise security attacks in IoT: Attacks, countermeasures, and open-issues. *Electronics*, *10*(19), 2365.

Wicaksono, D. (2022). *Sistem Keamanan Jaringan Menggunakan Firewall Dengan Metode Port Blocking Dan Firewall Filtering* (Doctoral dissertation, JATISI).

Wulan, W., Hadita, H., Fauzi, A., Putri, A. M., Fitriyani, F., Astriyani, R., ... & Cahyani, Y. I. (2024). Tinjauan Ancaman dan Risiko pada Sistem Keamanan Internet of Things, Berbasis Cloud Computing dalam Penggunaan E-Commerce dan Rencana Strategis. *Jurnal Kewirausahaan dan Multi Talenta*, *2*(2), 126-137.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada mahasiswa Teknik Informatika STMIK Widya Cipta Dharma yang telah kooperatif dalam penelitian ini. Terutama, kami berterima kasih kepada kampus STMIK Widya Cipta Dharma yang senantiasa mendukung kegiatan penelitian para dosen baik melalui dukungan finansial, materil dan non-materil