DAFTAR PUSTAKA

[1] M. Dehan Pratama, F. Nova, and D. Prayama, "Wazuh sebagai Log Event Management dan Deteksi Celah Keamanan pada Server dari Serangan Dos," *Jurnal Ilmiah Teknologi Sistem Informasi*, vol. 3, no.1, 2022.

[2] M. Nas, F. Ulfiah, U. Putri, T. Elektro, P. Negeri, and U. Pandang, "Analisis Sistem Security Information and Event Management (SIEM) Aplikasi Wazuh pada Dinas Komunikasi Informatika Statistik dan Persandian Sulawesi Selatan," *Jurnal Teknologi Elekterika*, vol. 20, no. 2, 2023.

[3] Stanković S, Gajin S, and Petrović R, "A Review of Wazuh Tool Capabilities for Detecting Attacks Based on Log Analysis," *Proceedings, Ix International Conference Icetran*, Jun. 2022, Accessed: Dec. 23, 2025. [Online]. Available: https://www.etran.rs/2022/zbornik/ICETRAN-22_radovi/068-RTI2.6.pdf

[4] Microsoft Security, "Apa Itu Pusat Operasi Keamanan (SOC)?," Microsoft. Accessed: Dec. 23, 2025. [Online]. Available: https://www.microsoft.com/id-id/security/business/security-101/what-is-a-security-operations-center-soc

[5] R. Aditya, Y. Muhyidin, and D. Singasatia, "Implementasi Security Information And Event Management (SIEM) Untuk Monitoring Keamanan Server Menggunakan Wazuh," *Jurnal Riset Sistem Informasi dan Teknik Informatika*, vol. 2, no. 5, 2024, doi: 10.61132/merkurius.v2i4.289.

[6] S. ardy Nuswantoro, M. Ziaurrahman, M. Miftahurrizqi, M. Achiril Haq, and R. A. Rashid, "Implementasi Wazuh-ELK-Suricata untuk Deteksi Privilege Escalation di Ubuntu Server," *Jurnal SAINTEKOM*, vol. 15, no. 2, pp. 153–164, Sep. 2025, doi: 10.33020/saintekom.v15i2.941.

[7] I. Bisnis Muhammadiyah Bekasi, S. Candra Kusuma, Y. Fadhillah Soleman, B. Berlinton, and S. Karya, "A Siem-Driven Solution For Cyber Attack Detection In Educational Websites: Implementing Threat Log Filtering For Enhanced Security," *JUPITER Teknologi Informatika & Komputer*, vol. 6, no. 1, 2025.

[8] Gede Parama Antara and Ika Dyah Agustia Rachmawati, "Implementasi dan Analisis Wazuh Sebagai Intrusion Detection System (IDS) dan Platform

Monitoring," *Jurnal Informasi, Sains dan Teknologi*, vol. 7, no. 2, pp. 290–303, Dec. 2024, doi: 10.55606/isaintek.v7i2.301.

[9] F. A. Saputra *et al.*, "Implementasi Wazuh Siem Untuk Manajemen Log Event Di Pesantren Teknologi Informasi Dan Komunikasi Jombang," *Jurnal Informatika Terpadu*, vol. 10, no. 2, pp. 146–155, 2024, [Online]. Available: https://journal.nurulfikri.ac.id/index.php/JIT

[10] M. Irdian Saputra and J. A. Yani, "Literature Review Network Security," 2023.

[11] A. Irfan, A. Z. Nusri, Z. Rachmat, and S. Wulandari, "Analisis Keamanan Jaringan Nirkabel Menggunakan Wireless Intrusion Detection System (WIDS)," *Jurnal Ilmiah Sistem Informasi dan Teknik Informatika (JISTI)*, vol. 7, no. 1, pp. 110–119, Apr. 2024, doi: 10.57093/jisti.v7i1.195.

[12] A. Bilal, Z. Veleučilište, B. Zaprešić, and C. M. Kalamir, "Strategic Approaches to Cybersecurity: The Role of the Security Operations Center," *Croatian Regional Development Journal* |, vol. 6, no. 2, 2025, doi: 10.2478/crdj-2025-0007.

[13] R. Fadholi and R. F. Aji, "Perancangan Kapabilitas Security Operations Center di Public Cloud Computing Environment: Studi Kasus PT. XYZ," *The Indonesian Journal of Computer Science*, 2025.

[14] M. Al Amin and R. Rahman, "Implementasi Security Information And Event Management (SIEM) Dalam Meningkatkan Keamanan Jaringan," *JURTIKOM*, vol. 1, no. 3, 2024, doi: 10.69714/ee1r1q05.

[15] K. Bezas and F. Filippidou, "Comparative Analysis of Open Source Security Information & Event Management Systems (SIEMs)," *Indonesian Journal of Computer Science*, 2023, Accessed: Jan. 03, 2026. [Online]. Available: https://doi.org/10.33022/ijcs.v12i2.3182

[16] D. D. Sahara, S. ; Sapri, and A. Akbar, "The Design And Implementation Of Computer Network Monitoring And Security System Using Linux Ubuntu Server," ARTICLE HISTORY, 2024.

[17] A. Prana Walidin *et al.*, "Kali Linux Sebagai Alat Analisis Keamanan Jaringan Melalui Penggunaan Nmap, Wireshark, Dan Metasploit," 2025.

[18] M. F. Zulfi, O. Alvansyah, A. Y. Al-Hafiz, and D. Kiswanto, “Pengujian Keamanan Jaringan Menggunakan Kali Linux Di Lingkungan Google Cloud Platform,” 2025.

[19] Alexander S. Gillis, “What is a Private IP Address?” Accessed: Jan. 12, 2026. [Online]. Available: https://www.techtarget.com/whatis/definition/private-IP-address

[20] E. Farrier, “Private vs. Public IP Addresses | Differences Explained.” Accessed: Jan. 12, 2026. [Online]. Available: https://www.avast.com/c-ip-address-public-vs-private

[21] Adam Zukhruf, Bagus Fatkhurrozi, and Andriyatna Agung Kurniawan, “Comparative Study Of Distributed Denial Of Service (DDoS) Attack Detection In Computer Networks,” *Jurnal Teknik Informatika (Jutif)*, vol. 4, no. 5, pp. 1033–1039, Oct. 2023, doi: 10.52436/1.jutif.2023.4.5.756.

[22] F. Nisa and S. Ramadona, “Sistem Pencegahan Serangan Distributed Denial Of Service Pada Jaringan SDN,” *Jurnal Sistim Informasi dan Teknologi*, vol. 5, no. 3, 2023, doi: 10.60083/jsisfotek.v5i3.269.

[23] P. Balqis and R. Rahman, “Analisis Keamanan Layanan SSH terhadap Brute Force Attack,” *Jurnal Riset Sistem Informasi dan Teknik Informatika*, vol. 3, no. 4, 2025, doi: 10.61132/merkurius.v3i4.949.

[24] A. P. Usman and R. Yusliana Bakti, “Optimalisasi Sistem Keamanan SSH dari Serangan Brute Force Menggunakan Intrusion Prevention System pada Mikrotik,” *Arus Jurnal Sains dan Teknologi(AJST)*, vol. 2, no. 1, 2024, [Online]. Available: http://jurnal.ardenjaya.com/index.php/ajsthttp://jurnal.ardenjaya.com/index.php/ajst

[25] M. Irfa’issurur and B. P. Josaphat, “Machine Learning for Cybersecurity: Web Attack Detection (Brute Force, XSS, SQL Injection),” *InPrime: Indonesian Journal of Pure and Applied Mathematics*, vol. 7, no. 1, pp. 1–15, Feb. 2025, doi: 10.15408/inprime.v7i1.41025.

[26] A. Suryadin, K. A. Latif, L. Widyawati, R. Azhar, and M. Azwar, “Evaluasi Penerapan Pertahanan Proaktif Waf Dan Hids Terhadap Eksploitasi Kerentanan Aplikasi Web,” Mataram, Sep. 2025.

[27] I. M. Razzanda and M. Koprawi, “Implementasi IDS dan IPS terhadap Serangan TCP Port Scanning dan ICMP Flooding,” *The Indonesian Journal of Computer Science*, vol. 13, no. 4, 2024.

[28] M. Suhaidi and N. Nurhadi, “Implementasi dan Analasis Keamanan Jaringan Pada STIA Lancang Kuning Dumai Menggunakan Port Scanning dan Firewall Tarpit,” *Arcitech: Journal of Computer Science and Artificial Intelligence*, vol. 3, no. 2, p. 110, Dec. 2023, doi: 10.29240/arcitech.v3i2.8181.

[29] M. R. Adha, “Analisis Perbandingan Kinerja Aplikasi Web Browser Bardasarkan Sistem Operasi,” Skripsi, Universitas Islam Negeri Ar-Raniry, Banda Aceh, 2023.

[30] R. R. Chand, N. A. Sharma, and M. A. Kabir, “Advancing Web Browser Forensics: Critical Evaluation of Emerging Tools and Techniques,” *SN Comput. Sci.*, vol. 6, no. 4, Apr. 2025, doi: 10.1007/s42979-025-03921-6.

[31] Y. Sopyan and M. Rovi, “Implementasi Metode Ndlc Pada Infrastruktur Jaringan Universitas Bhakti Husada Indonesia Dengan Memanfaatkan Whatsapp Gateway Sebagai Monitoring,” *INFOTECH journal*, vol. 11, no. 2, pp. 174–183, Jul. 2025, doi: 10.31949/infotech.v11i2.14835.

[32] D. Saputra and B. Y. Geni, “Analisa Dan Perancangan Jaringan Wireless Local Area Network (WLAN) Dengan Menggunakan Metode NDLC (Studi Kasus : Di Toko Besi Kunciran Baja),” *JATI(Jurnal Mahasiswa Teknik Informatika)*, vol. 8, 2024.

[33] Cherilyn Pascoe, Stephen Quinn, and Karen Scarfone, “The NIST Cybersecurity Framework (CSF) 2.0,” Feb. 2024. doi: 10.6028/NIST.CSWP.29.

[34] Windari Ratih and Sriyanto, “TINJAUAN IMPLEMENTASI NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) DALAM MENINGKATKAN KEAMANAN JARINGAN DENGAN CYBERSECURITY FRAMEWORK (CSF) : STUDI KASUS SMKN4 BANDAR LAMPUNG,” *Jurnal Ilmu Komputer, Sistem Informasi, Teknik Informatika*, vol. 3, no. 1, pp. 2964–4763, 2024.