DAFTAR PUSTAKA

[1] G. Shanmugarathinam, A. G. Jesudoss, A. Joseph, K. Yadav, and A. Shashidar, “Enhance the Network Security in Enterprise Network Using IDPS Tools,” in *2025 2nd International Conference on New Frontiers in Communication, Automation, Management and Security*, pp. 1–5, 2025, doi: 10.1109/ICCAMS65118.2025.11234631.

[2] B. R. Utomo, N. H. Jati, A. K. Jati, I. A. Saputro, and M. H. Purwidiantoro, “Analisis Implementasi Keamanan Jaringan dengan Fail2Ban terhadap Serangan Bruteforce,” *Prosiding Seminar Nasional AMIKOM Surakarta*, vol. 2, pp. 1211–1223, 2024.

[3] R. K. Abdullah, M. T. Fudhail, and S. Mujahidin, “Penggunaan Snort dan Fail2Ban sebagai IDS untuk Mengatasi Brute Force Attack dengan Notifikasi Telegram: Studi Kasus pada Institusi XYZ,” *Jurnal Sistem dan Teknologi Informasi*, vol. 12, no. 3, p. 530, 2024, doi: 10.26418/justin.v12i3.79617.

[4] D. R. Juliandi, J. Karman, and Rusdiyanto, “Perancangan Sistem Bot Alert Telegram sebagai Notifikasi Deteksi Serangan Ping of Death Berbasis Snort,” *RESOLUSI: Rekayasa Teknik Informatika dan Informasi*, vol. 5, no. 1, pp. 49–57, 2024, doi: 10.30865/resolusi.v5i1.2168.

[5] K. M. S. Kursheeth, T. Sree, D. S. Vadivu, Y. S. S. Harsha, and N. Rajagopalan, “Suricata-Based Intrusion Detection and Isolation System for Local Area Networks,” in *2024 International Conference on Signal Processing, Computation, Electronics, Power and Telecommunication*, pp. 1–5, 2024, doi: 10.1109/IConSCEPT61884.2024.10627890.

[6] M. Tahir, U. Wahyuningsih, M. I. P. Pratama, and M. A. Effindi, “Development of Network Security Using a Suricata-Based Intrusion Prevention System Against Distributed Denial of Service,” *Innovation Research in Informatics*, vol. 6, no. 2, pp. 41–48, 2024, doi: 10.37058/innovatics.v6i2.11187.

[7] A. A. E. Boukebous, M. I. Fettache, G. Bendiab, and S. Shiaeles, “A Comparative Analysis of Snort 3 and Suricata,” in *2023 IEEE IAS Global*

Conference on Emerging Technologies, pp. 1–6, 2023, doi: 10.1109/GlobConET56651.2023.10150141.

[8] R. Yalda, N. Nepal, and T. El Hawari, "Enhancing IoT Security Affordably with Raspberry Pi and Open-Source IDS/IPS," in *2024 IEEE International Conference on Advanced Systems and Emergent Technologies*, pp. 1–6, 2024, doi: 10.1109/IC_ASET61847.2024.10596202.

[9] D. F. Priambodo, Amiruddin, and N. Trianto, "Hardening a Work from Home Network with WireGuard and Suricata," in *Proceedings of the 2nd International Conference on Computer Science and Engineering*, pp. 1–4, 2021, doi: 10.1109/IC2SE52832.2021.9791983.

[10] M. Vasilakis, M. Tampouratzis, and A. Dimitriadis, "Integrated Threat Intelligence and Event Correlation with Wazuh, Suricata, and MISP," in *2025 6th International Conference on Communications, Information, Electronic and Energy Systems*, pp. 1–5, 2025, doi: 10.1109/CIEES66347.2025.11300009.

[11] D. H. K. Raharjo, A. Nurmala, R. D. Pambudi, and R. F. Sari, "Performance Evaluation of Intrusion Detection System for Traffic Anomaly Detection Based on Active IP Reputation Rules," in *Proceedings of the International Conference on Electrical Engineering and Informatics*, pp. 75–79, 2022, doi: 10.1109/IConEEI55709.2022.9972298.

[12] H. Vaghela and V. Khirasaria, "Securing Private Blockchain Infrastructures: Detection and Prevention of DDoS Attacks Using Suricata," in *2024 Parul International Conference on Engineering and Technology*, pp. 1–5, 2024, doi: 10.1109/PICET60765.2024.10716201.

[13] N. Ragavenderan, S. U. R., and R. K. P., "AI-Powered Adaptive Firewall Using Suricata and Large Language Models," in *2025 9th International Conference on Computational Systems and Information Technology for Sustainable Solutions*, pp. 1–5, 2025, doi: 10.1109/CSITSS67709.2025.11295292.

[14] F. S. Sulaiman, H. B. Seta, and N. Falih, "Exploitation Prevention on Network Printer with Signature-Based Suricata on pfSense," in *Proceedings of the 3rd International Conference on Informatics, Multimedia, Cyber and*

Information System, pp. 35–39, 2021, doi: 10.1109/ICIMCIS53775.2021.9699133.

[15] Z. Bakraouy, W. Abbass, M. Boughanja, M. Flissat, A. Baina, and M. Bellafkih, "Hybrid NIDS Architecture Leveraging Suricata, Zeek and the ELK Stack," in *2025 International Conference on Intelligent Systems: Theories and Applications*, pp. 1–7, 2025, doi: 10.1109/SITA67914.2025.11273397.

[16] C. P. Nwankwo et al., "Improving Open-Source Network Security Tooling for the Corporate Enterprise," in *IEEE International Conference on Emerging and Sustainable Technologies for Power and ICT in a Developing Society*, pp. 1–5, 2024, doi: 10.1109/NIGERCON62786.2024.10927387.

[17] P. Chinnasamy, C. Sivakrishnaiah, T. Anjali, A. Kambalapelly, P. V. Rao, and D. P. Degala, "Managing Network Security in IT Sector Using Suricata," in *Proceedings of the 3rd International Conference on Self Sustainable Artificial Intelligence Systems*, pp. 1721–1728, 2025, doi: 10.1109/ICSSAS66150.2025.11080990.

[18] C. Zlatea, E. Resul, and J. A. Văduva, "Monitoring Wireless Networks Using a Low-Cost, Decoupled ESP32-Based Architecture," in *Proceedings of the RoEduNet IEEE International Conference*, pp. 1–4, 2025, doi: 10.1109/RoEduNet68395.2025.11208386.

[19] N. C. Sari, A. Solichan, B. Ansor, A. P. Ramdani, M. Z. Al Amin, M. Khaira, and A. R. R. Al Ubaidah, "Deteksi Kerentanan SQL Injection pada Website Menggunakan Vulnerability Assessment," *Journal of Data Insights*, vol. 2, no. 1, pp. 9–17, 2024, doi: 10.26714/jodi.v2i1.393.

[20] A. Gustiyono, E. I. Alwi, and S. M. Abdullah, "Analisa Kerentanan Website terhadap Serangan Cross-Site Scripting (XSS) Metode Penetration Testing," *CyberSecurity dan Forensik Digital*, vol. 7, no. 1, pp. 25–33, 2024.

[21] T. Ariyadi, M. A. Nuriansyah, E. Rahmadan, and D. Saputra, "Keamanan FTP Server Berbasiskan IPS Menggunakan Sistem Operasi Linux Ubuntu Versi 24.04," *Jurnal Penelitian Multidisiplin Bangsa*, vol. 2, no. 1, pp. 49–55, 2025, doi: 10.59837/jpnmb.v2i1.428.

[22] Z. I. Sumayyah, S. D. S. Permana, M. Tsabit, and A. Setiawan, “Penerapan dan Mitigasi Teknik Slowloris dalam Serangan Distributed Denial-of-Service (DDoS) terhadap Website Ilegal dengan Kali Linux,” *Journal of Internet and Software Engineering*, vol. 1, no. 2, pp. 1–14, 2024.

[23] R. Laipaka, Busriki, and A. Della, “Pengujian Keamanan Website Menggunakan Kali Linux dan Nikto untuk Mengetahui Kerentanan,” in *Seminar Nasional CORISINDO*, STMIK Pontianak, pp. 71–76, 2023.

[24] Y. Muhyidin, M. H. Totohendarto, E. Undamayanti, and S. Choerunnisa, “Perbandingan Tingkat Keamanan Website Menggunakan Nmap dan Nikto dengan Metode Ethical Hacking,” *Jurnal Teknologika*, vol. 12, no. 1, pp. 80–89, 2022, doi: 10.51132/teknologika.v12i1.143.

[25] Yunanri W., Yuliadi, F. Hamdani, Y. B. Fitriana, and N. Oper, “Analisis Keamanan Website terhadap Serangan DDoS Menggunakan Metode National Institute of Standards and Technology (NIST),” *KLIK: Kajian Ilmiah Informatika dan Komputer*, vol. 3, no. 6, pp. 1296–1302, 2023, doi: 10.30865/klik.v3i6.830.

[26] M. I. Sabila, M. Tahir, S. D. Mardania, and R. I. Arifin, “Implementasi Snort sebagai IDS dalam Mendeteksi Serangan Port Scanning Nmap pada Simulasi Jaringan Virtual,” *JATI: Jurnal Mahasiswa Teknik Informatika*, vol. 9, no. 4, pp. 6944–6950, 2025.

[27] K. S. M. Wikrama, R. Firdaus, L. Z. M. Mendrofa, G. A. J. Saskara, and I. M. E. Listartha, “DDoS Attack Using GoldenEye, DAVOSET, and PyLoris Tools,” *Jurnal CoreIT*, vol. 9, no. 2, pp. 43–52, 2023, doi: 10.24014/coreit.v9i2.20020.

[28] R. A. Puspita D., P. D. Persadha, and Mulyadi, “Analisis Ancaman Serangan Siber pada Infrastruktur Informasi Vital terhadap Stabilitas Keamanan Nasional,” *Syntax Literate: Jurnal Ilmiah Indonesia*, vol. 10, no. 5, pp. 5397–5406, 2025.

[29] L. T. Sontani, A. Budiono, and A. Widjajarto, “Implementasi dan Analisis Sistem Forensik Digital pada Linux Vulnerable Machine Menggunakan Framework Forensics Zachman,” *Journal of Production, Enterprise, and*

Industrial Applications, vol. 2, no. 2, pp. 1–6, 2024, doi: 10.25124/jpeia.v2i2.8721.

[30] W. S. Raharjo and A. A. Bajuadji, "Analisa Implementasi Protokol HTTPS pada Situs Web Perguruan Tinggi di Pulau Jawa," *ULTIMATICS*, vol. 8, no. 2, pp. 102–111, 2016.

[31] T. Dai, S. Ray, L. M. Ellram, C. Tang, J. Sarkis, R. B. Handfield, J. G. Roehrich, and M. Stoyanova, "Identification, Tracking and Disruption of Covert Supply Chain Operations: A Research Agenda," *International Journal of Operations & Production Management*, pp. 233–252, 2025, doi: 10.1108/IJOPM-02-2025-0115.

[32] A. Rustianto, A. Fadillah, and J. Kasih, "Pencegahan dan Visualisasi Serangan Brute Force Menggunakan Fail2Ban, Prometheus, dan Grafana: Studi Kasus di Sekolah Tinggi Teknologi Terpadu Nurul Fikri," *Jurnal Publikasi Teknik Informatika*, vol. 4, no. 2, pp. 195–209, 2025, doi: 10.55606/jupti.v4i2.5144.

[33] P. Balqis and R. Rahman, "Analisis Keamanan Layanan SSH terhadap Brute Force Attack," *Merkurius: Jurnal Riset Sistem Informasi dan Teknik Informatika*, vol. 3, no. 4, pp. 240–246, 2025, doi: 10.61132/merkurius.v3i4.949.

[34] S. A. Valianta, Tasmi, and D. Stiawan, "Identifikasi Serangan Port Scanning dengan Metode String Matching," *Prosiding Annual Research Seminar*, vol. 2, no. 1, pp. 466–471, 2016.

[35] W. Septriyanti, "Pembaharuan Sistem Deteksi Serangan Portscan Berbasis LSTM dengan Pengimplementasian Algoritma Unidirectional LSTM (UNI-LSTM)," Skripsi, Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya, 2023.

[36] D. Y. Zebua, C. S. C. Waruwu, K. Zebua, M. Zai, A. Lase, and O. Laia, "Simulasi Serangan DoS Menggunakan SlowHTTPTest," *JUKTISI*, vol. 4, no. 2, pp. 409–419, 2025, doi: 10.62712/juktisi.v4i2.402.

[37] K. Sussolaikah, P. Adytia, Wahyuni, and L. A. Rahmi, "Identifikasi Serangan DDoS pada Jaringan Komputer Menggunakan Algoritma

Artificial Neural Network," *Neptunus: Jurnal Ilmu Komputer dan Teknologi Informasi*, vol. 1, no. 1, pp. 1–11, 2023, doi: 10.61132/neptunus.v1i1.67.

[38] W. Wahyat and P. Kudadiri, "Implementation of Intrusion Detection System With Suricata on Ubuntu 22.04 LTS," *Jurnal Teknologi Elekterika*, vol. 21, no. 1, pp. 50–53, 2024.