DAFTAR PUSTAKA

[1] Pengguna internet di Indonesia meningkat pesat, capai 221 juta orang di tahun 2024," *Smart City Gunungkidul*, 14 Februari 2024. [Online]. Tersedia: https://smartcity.gunungkidulkab.go.id/2024/02/14/pengguna-internet-di-indonesia-meningkat-pesat-capai-221-juta-orang-di-tahun-2024/. [Diakses: 13-Jan-2025].

[2] A. Wijayanto, I. Riadi, and Y. Prayudi, "TAARA Method for Processing on the Network Forensics in the Event of an ARP Spoofing Attack," Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi), vol. 7, no. 2, pp. 208–217, 2023.

[3] S. Syaifuddin and D. R. Akbi, "Analisis Address Resolution Protocol Poisoning Attack Pada Router WLAN Menggunakan Metode Live Forensics," *Jurnal Komputer Terapan*, vol. 7, no. 1, pp. 62–73.

[4] A. Alsaaidah, O. Almomani, A. A. Abu-Shareha, M. M. Abualhaj, and A. Achuthan, "ARP spoofing attack detection model in IoT network using machine learning: Complexity vs. accuracy," *Journal of Applied Data Sciences*, vol. 5, no. 4, pp. 1850–1860, 2024.

[5] L. Breiman, "Random Forest s," Machine Learning, vol. 45, no. 1, pp. 5–32, 2001.

[6] 1 N. Ahuja, G. Singal, D. Mukhopadhyay, and A. Nehra, "Ascertain the efficient machine learning approach to detect different ARP attacks," *Computers and Electrical Engineering*, vol. 99, p. 107757, 2022,

[7] D. R. Thomas, W. Nancy, G. Sowmiya, T. P. Adhithya, and V. Peroumal, "Detection and prevention of poisoning targets with ARP cache using Scapy," in *2024 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE)*, Jan. 2024, pp. 1–6.

[8] S. Kumar and P. Dash, "Detecting and Preventing ARP Spoofing Attacks Using Real-Time Data Analysis and Machine Learning," *Journal of Cybersecurity Research*, 2024.

[9] P. C. Nguyen, Q. T. Nguyen, and K. H. Le, "An ensemble feature selection algorithm for machine learning based intrusion detection system," in *2021 8th NAFOSTED Conf. on Inf. and Comput. Sci. (NICS)*, Dec. 2021, pp. 50-54, IEEE.

[10] S. Majumder, M. K. Deb Barma, dan A. Saha, "ARP spoofing detection using machine learning classifiers: an experimental study," Knowl. Inf. Syst., vol. 2024, 2024. doi: 10.1007/s10115-024-02219-y.

[11] S. Kumar, R. Singh, and M. A. Al-Zubi, "Performance enhancement of wireless networks: A survey of smart techniques and enabling methodologies," Computer Communications, vol. 173, pp. 68–90, Mar. 2021. DOI: 10.1016/j.comcom.2021.03.018.

[12] W. Chong, H. Wang, and Z. Liu, "Integration of IoT with WLAN: A systematic review and future directions," IEEE Access, vol. 8, pp. 123456–123470, Jan. 2020. DOI: 10.1109/ACCESS.2020.2968812.

[13] "Types of Hackers: Black Hat, White Hat and Grey Hat Explained," Kaspersky Resource Center, [Online]. Available: https://www.kaspersky.com/resource-center/definitions/hacker-hat-types. [Accessed: 18-Jan-2025].

[14] B. Dodiya and U. K. Singh, "Malicious Traffic Analysis using Wireshark by Collection of Indicators of Compromise," *International Journal of Computer Applications*, vol. 183, no. 53, pp. 1–6, Feb. 2022.

[15] A. F. A. H. Alnuaimi and T. H. K. Albaldawi, "An overview of machine learning classification techniques," *BIO Web of Conferences*, vol. 97, Art. no. 00133, 2024. [Online]. Available: https://doi.org/10.1051/bioconf/20249700133

[16] O. Rainio, J. Teuho, and R. Klén, "Evaluation metrics and statistical tests for machine learning," Sci. Rep., vol. 14, no. 1, p. 6086, 2024.

[17] F. Martínez-Plumed, L. Contreras-Ochando, C. Ferri, J. Hernández-Orallo, M. Kull, N. Lachiche, M. J. Ramírez-Quintana, and P. Flach, "CRISP-DM Twenty Years Later: From Data Mining Processes to Data Science Trajectories," IEEE Transactions on Knowledge and Data Engineering, vol. 33, no. 8, pp. 3048–3061, Aug. 2021, doi: 10.1109/TKDE.2019.2962680.

[18] H. Patel, D. S. Rajput, G. T. Reddy, C. Iwendi, A. K. Bashir, and O. Jo, "A review on classification of imbalanced data for wireless sensor networks," *Int. J. Distrib. Sensor Networks*, vol. 16, no. 4, 2020, Art. no. 1550147720916404. doi: 10.1177/1550147720916404.

[19] J. Hatwell, M. M. Gaber, and R. M. Atif Azad, "Ada-WHIPS: Explaining AdaBoost classification with applications in the health sciences," BMC Medical Informatics and Decision Making, vol. 20, pp. 1–25, 2020.

[20] C. Schröer, F. Kruse, and J. M. Gómez, "A systematic literature review on applying CRISP-DM process model," Procedia Computer Science, vol. 181, pp. 526-534, 2021.

[21] C. E. Durango Vanegas, J. C. Giraldo Mejía, F. A. Vargas Agudelo, and D. E. Soto Duran, "A representation based on essence for the CRISP-DM methodology," Computación y Sistemas, vol. 27, no. 3, pp. 675-689, 2023.

[22] V. C. B. Ginting, M. Data, and D. P. Kartikasari, "Deteksi Serangan ARP Spoofing berdasarkan Analisis Lalu Lintas Paket Protokol ARP," *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, vol. 3, no. 5, pp. 5049–5057, 2019.

[23] A. A. Galal, A. Z. Ghalwash, and M. Nasr, "A new approach for detecting and mitigating address resolution protocol (ARP) poisoning," *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 6, 2022.

[24] L. Patrice, R. Sinde, and J. Leo, "A novel mechanism for detection of address resolution protocol spoofing attacks in large-scale software-defined networks," *IEEE Access*, vol. 12, pp. 80255–80265, 2024.

Halaman ini sengaja dikosongkan