# DAFTAR PUSTAKA


[1] S. Chandran, S. R. Syam, S. Sankaran, T. Pandey, and K. Achuthan, "From Static to AI-Driven Detection: A Comprehensive Review of Obfuscated Malware Techniques," *IEEE Access*, vol. 13, pp. 74335–74358, 2025, doi: 10.1109/ACCESS.2025.3550781.

[2] P. Caporaso, G. Bianchi, and F. Quaglia, "JITScanner: Just-in-Time Executable Page Check in the Linux Operating System," *Appl. Sci.*, vol. 14, no. 5, p. 1912, Jan. 2024, doi: 10.3390/app14051912.

[3] D. Hermawan, M. Z. Mutaqim, T. Hidayat, and A. H. Anshor, "KEAMANAN KERNEL PADA SISTEM OPERASI MODERN," vol. 9, no. 2, 2025.

[4] S. N. A. Sherazi and A. Qureshi, "Hybrid Analysis Model for Detecting Fileless Malware," *Electronics*, vol. 14, no. 15, p. 3134, Aug. 2025, doi: 10.3390/electronics14153134.

[5] I. Kara, "Fileless malware threats: Recent advances, analysis approach through memory forensics and research challenges," *Expert Syst. Appl.*, vol. 214, p. 119133, Mar. 2023, doi: 10.1016/j.eswa.2022.119133.

[6] Y. Takabayashi and M. Mambo, "Detection Evasion Using eBPF for Linux Fileless Malware," in *2024 IEEE Conference on Dependable and Secure Computing (DSC)*, Tokyo, Japan: IEEE, Nov. 2024, pp. 74–75. doi: 10.1109/DSC63325.2024.00026.

[7] M. Hanchenko, "Analysis Of Methods For Detecting Fileless Malware In The Energy-Dependent Memory Of An Organisation's Information System Assets," in *Ricerche Scientifiche E Metodi Della Loro Realizzazione: Esperienza Mondiale E Realtà Domestiche*, European Scientific Platform, Apr. 2024. doi: 10.36074/logos-26.04.2024.054.

[8] M.-H. Wu *et al.*, "Enhancing Linux System Security: A Kernel-Based Approach to Fileless Malware Detection and Mitigation," *Electronics*, vol. 13, no. 17, p. 3569, Jan. 2024, doi: 10.3390/electronics13173569.

[9] S. M. L. Lima *et al.*, "Next-generation antivirus endowed with web-server Sandbox applied to audit fileless attack," *Soft Comput.*, vol. 27, no. 3, pp. 1471–1491, Feb. 2023, doi: 10.1007/s00500-022-07447-4.

[10] R. Tóth, T. Bisztray, and L. Erdődi, "LLMs in Web Development: Evaluating LLM-Generated PHP Code Unveiling Vulnerabilities and Limitations," in *Computer Safety, Reliability, and Security. SAFECOMP 2024 Workshops*, vol. 14989, A. Ceccarelli, M. Trapp, A. Bondavalli, E. Schoitsch, B. Gallina, and F. Bitsch, Eds., in Lecture Notes in Computer

Science, vol. 14989. , Cham: Springer Nature Switzerland, 2024, pp. 425–437. doi: 10.1007/978-3-031-68738-9_34.

[11] J. Ramamoorthy, K. Gupta, R. C. Kafle, N. K. Shashidhar, and C. Varol, “A Novel Static Analysis Approach Using System Calls for Linux IoT Malware Detection,” *Electronics*, vol. 13, no. 15, p. 2906, July 2024, doi: 10.3390/electronics13152906.

[12] S.-H. Han and D. Lee, “Kernel-Based Real-Time File Access Monitoring Structure for Detecting Malware Activity,” *Electronics*, vol. 11, no. 12, p. 1871, June 2022, doi: 10.3390/electronics11121871.

[13] H. Wang, A. Yu, L. Xiao, J. Li, and X. Cao, “SPRT: Automatically Adjusting SELinux Policy for Vulnerability Mitigation,” in *Proceedings of the 29th ACM Symposium on Access Control Models and Technologies*, San Antonio TX USA: ACM, June 2024, pp. 71–82. doi: 10.1145/3649158.3657306.

[14] M. Miki, T. Yamauchi, and S. Kobayashi, “Effectiveness of MAC Systems based on LSM and their Security Policy Configuration for Protecting IoT Devices,” *J. Internet Serv. Inf. Secur.*, vol. 14, no. 3, pp. 293–315, Aug. 2024, doi: 10.58346/JISIS.2024.I3.018.

[15] W. Zhang, P. Liu, and T. Jaeger, “Analyzing the Overhead of File Protection by Linux Security Modules,” in *Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security*, Virtual Event Hong Kong: ACM, May 2021, pp. 393–406. doi: 10.1145/3433210.3453078.

[16] M. Abbadini, M. Beretta, D. Facchinetti, G. Oldani, M. Rossi, and S. Paraboschi, “Lightweight Cloud Application Sandboxing,” in *2023 IEEE International Conference on Cloud Computing Technology and Science (CloudCom)*, Naples, Italy: IEEE, Dec. 2023, pp. 139–146. doi: 10.1109/CloudCom59040.2023.00033.

[17] L. Alexander, “From Traditional Models To Zero-Trust: A Comparative Study Of Access Control Systems With Fast Monitor,” 2025.

[18] J. M. Delbugio and V. K. Madisetti, “Enhanced Memory-Safe Linux Security Modules (eLSMs) for Improving Security of Docker Containers for Data Centers,” *J. Softw. Eng. Appl.*, vol. 17, no. 05, pp. 259–269, 2024, doi: 10.4236/jsea.2024.175015.

[19] T. Dunlap, W. Enck, and B. Reaves, “A Study of Application Sandbox Policies in Linux,” in *Proceedings of the 27th ACM on Symposium on Access Control Models and Technologies*, New York NY USA: ACM, June 2022, pp. 19–30. doi: 10.1145/3532105.3535016.

[20] A. Niemi, “Survey of Real-World Process Sandboxing,” in *2024 35th Conference of Open Innovations Association (FRUCT)*, Tampere, Finland: IEEE, Apr. 2024, pp. 520–531. doi: 10.23919/FRUCT61870.2024.10516417.

[21] X. Yu, W. Meng, Y. Liu, and F. Zhou, “TridentShell: An enhanced covert and scalable backdoor injection attack on web applications,” *J. Netw. Comput. Appl.*, vol. 223, p. 103823, Mar. 2024, doi: 10.1016/j.jnca.2023.103823.

[22] O. Khalid *et al.*, “An Insight into the Machine-Learning-Based Fileless Malware Detection,” *Sensors*, vol. 23, no. 2, p. 612, Jan. 2023, doi: 10.3390/s23020612.

[23] A. Mujtaba, M. Zulfiqar, M. U. Azhar, S. Ali, A. Ali, and H. Khan, “ML-based Fileless Malware Threats Analysis for the Detection of Cyber security Attack based on Memory Forensics: A Survey,” *Asian Bull. Big Data Manag.*, vol. 5, no. 1, pp. 1–14, Jan. 2025, doi: 10.62019/abbdm.v5i1.289.

[24] P. Caporaso, G. Bianchi, and F. Quaglia, “Jitscanner: Just-in-time executable page check in the linux operating system,” in *Proceedings of the 18th International Conference on Availability, Reliability and Security*, 2023, pp. 1–8.

[25] S. M. L. Lima *et al.*, “Next-generation antivirus endowed with web-server Sandbox applied to audit fileless attack,” *Soft Comput.*, vol. 27, no. 3, pp. 1471–1491, Feb. 2023, doi: 10.1007/s00500-022-07447-4.