DAFTAR PUSTAKA

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

[2] A. Mujtaba, M. Zulfiqar, M. U. Azhar, S. Ali, A. Ali, dan H. Khan, "ML-based *File*less 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, hlm. 1–14, Jan 2025, doi: 10.62019/abbdm.v5i1.289.

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

[4] A. T. Syed, M. C. Ghanem, E. Benkhelifa, dan F. I. Abro, "SPECTRE: A Hybrid System for an Adaptative and Optimised Cyber Threats Detection, Response and Investigation in Volatile Memory," 7 Januari 2025, *arXiv*: arXiv:2501.03898. doi: 10.48550/arXiv.2501.03898.

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

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

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

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

[9] M. Miki, T. Yamauchi, dan 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, hlm. 293–315, Agu 2024, doi: 10.58346/JISIS.2024.I3.018.

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

[11] W. Zhang, T. Jaeger, dan P. Liu, "Analyzing the Overhead of *File*system Protection Using Linux Security Modules," 27 Januari 2021, *arXiv*: arXiv:2101.11611. doi: 10.48550/arXiv.2101.11611.

[12] J. M. Delbugio dan 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. 5, hlm. 259–269, Mei 2024, doi: 10.4236/jsea.2024.175015.

[13] S.-H. Han dan D. Lee, "*Kernel*-Based Real-Time *File* Access Monitoring Structure for Detecting Malware Activity," *Electronics*, vol. 11, no. 12, hlm. 1871, Jun 2022, doi: 10.3390/electronics11121871.

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

[15] F.-H. Hsu *dkk.*, "A *Kernel*-Based Solution for Detecting and Preventing *File*less Malware on Linux," 23 Agustus 2023, *Computer Science and Mathematics*. doi: 10.20944/preprints202308.1562.v1.

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

[17] O. Khalid *dkk.*, "An Insight into the Machine-Learning-Based *File*less Malware Detection," *Sensors*, vol. 23, no. 2, hlm. 612, Jan 2023, doi: 10.3390/s23020612.

[18] M. Hanchenko, "ANALYSIS OF METHODS FOR DETECTING *FILE*LESS MALWARE IN THE ENERGY-DEPENDENT MEMORY OF AN ORGANISATION'S INFORMATION SYSTEM ASSETS," dalam *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.

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

[20] J. Ramamoorthy, K. Gupta, R. C. Kafle, N. K. Shashidhar, dan C. Varol, "A Novel Static Analysis Approach Using System Calls for Linux IoT Malware Detection," *Electronics*, vol. 13, no. 15, hlm. 2906, Jul 2024, doi: 10.3390/electronics13152906.

[21] M.-H. Wu *dkk.*, "Enhancing Linux System Security: A *Kernel*-Based Approach to *File*less Malware Detection and Mitigation," *Electronics*, vol. 13, no. 17, hlm. 3569, Sep 2024, doi: 10.3390/electronics13173569.

[22] R. Tóth, T. Bisztray, dan L. Erdodi, "LLMs in Web Development: Evaluating LLM-Generated PHP Code Unveiling Vulnerabilities and Limitations," 21 Mei 2024, *arXiv*: arXiv:2404.14459. doi: 10.48550/arXiv.2404.14459.

[23] S. N. A. Sherazi dan A. Qureshi, “Hybrid Analysis Model for Detecting *File*less Malware,” *Electronics*, vol. 14, no. 15, hlm. 3134, Agu 2025, doi: 10.3390/electronics14153134.

[24] A. Juneja, “RX-INT: A *Kernel* Engine for Real-Time Detection and Analysis of In-Memory Threats,” 5 Agustus 2025, *arXiv*: arXiv:2508.03879. doi: 10.48550/arXiv.2508.03879.

[25] L. Alexander, “FROM TRADITIONAL MODELS TO ZERO-TRUST: A COMPARATIVE STUDY OF ACCESS CONTROL SYSTEMS WITH FAST MONITOR,” 2025, Diakses: 15 September 2025. [Daring]. Tersedia pada: https://www.researchgate.net/pro*file*/Luna-Alexandra/publication/391839342_FROM_TRADITIONAL_MODELS_TO_ZERO-TRUST_A_COMPARATIVE_STUDY_OF_ACCESS_CONTROL_SYSTEMS_WITH_FAST_MONITOR/links/6828d88d6b5a287c30424778/FROM-TRADITIONAL-MODELS-TO-ZERO-TRUST-A-COMPARATIVE-STUDY-OF-ACCESS-CONTROL-SYSTEMS-WITH-FAST-MONITOR.pdf