

DAFTAR PUSTAKA

- [1] “LANSKAP KEAMANAN SIBER INDONESIA 2024.”
- [2] D. Singasatia, M. Kom, ; M Hafid Totohendarto, S. M. M. Si, J. Saputro, dan S. Kom, “PENETRATION TESTING UNTUK MENGUJI KERENTANAN PADA SISTEM INFORMASI AKADEMIK DI SEKOLAH TINGGI TEKNOLOGI XYZ.” [Daring]. Tersedia pada: <http://www.IANA.org>,
- [3] N. Koroniotis, N. Moustafa, B. Turnbull, F. Schiliro, P. Gauravaram, dan H. Janicke, “A Deep Learning-based Penetration Testing Framework for Vulnerability Identification in Internet of Things Environments,” dalam *Proceedings - 2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2021*, Institute of Electrical and Electronics Engineers Inc., 2021, hlm. 887–894. doi: 10.1109/TrustCom53373.2021.00125.
- [4] Jerry Gamblin, “2024 CVE Data Review.”
- [5] . Design, N. R. Rosyid, A. K. Fauziyyah, dan Y. N. Ananda, “Enhancing Cybersecurity: Design of an Automated Penetration Testing Framework for Common Vulnerabilities and Exposures (CVE),” 2025.
- [6] J.-P. A. Yaacoub, H. N. Noura, O. Salman, dan A. Chehab, “A Survey on Ethical Hacking: Issues and Challenges,” Mar 2021, [Daring]. Tersedia pada: <http://arxiv.org/abs/2103.15072>
- [7] C. Skandylas dan M. Asplund, “Automated Penetration Testing: Formalization and Realization,” Des 2024, [Daring]. Tersedia pada: <http://arxiv.org/abs/2412.12745>
- [8] E. Hilario, S. Azam, J. Sundaram, K. Imran Mohammed, dan B. Shanmugam, “Generative AI for pentesting: the good, the bad, the ugly,” *Int J Inf Secur*, vol. 23, no. 3, hlm. 2075–2097, Jun 2024, doi: 10.1007/s10207-024-00835-x.
- [9] G. Deng dkk., *PentestGpt: Evaluating and Harnessing Large Language Models for Automated Penetration Testing*. [Daring]. Tersedia pada: <https://www.usenix.org/conference/usenixsecurity24/presentation/deng>

- [10] M. Patil, D. Thakare, A. Bhure, S. Kaundanyapure, dan Dr. A. Mune, “An AI-Based Approach for Automating Penetration Testing,” *Int J Res Appl Sci Eng Technol*, vol. 12, no. 4, hlm. 5019–5028, Apr 2024, doi: 10.22214/ijraset.2024.61113.
- [11] Siva Krishna Jampani, “Revolutionizing Penetration Testing: AI-Powered Automation for Enterprise Security,” *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, vol. 10, no. 6, hlm. 1562–1569, Des 2024, doi: 10.32628/cseit241061201.
- [12] A. L. Martínez, A. Cano, dan A. Ruiz-Martínez, “Generative Artificial Intelligence-Supported *Pentesting*: A Comparison between Claude Opus, GPT-4, and Copilot,” Jan 2025, [Daring]. Tersedia pada: <http://arxiv.org/abs/2501.06963>
- [13] I. Kecerdasan Buatan Generatif Untuk Analisis dan, P. Putra Abimata, dan M. Andri Setiawan, “Copyright © KESATRIA: Jurnal Penerapan Sistem Informasi (Komputer & Manajemen),” 2024.
- [14] W. Zhang, J. Xing, dan X. Li, “Penetration Testing for System Security: Methods and Practical Approaches,” Mei 2025, [Daring]. Tersedia pada: <http://arxiv.org/abs/2505.19174>
- [15] National Institute of Standards and Technology, “Penetration Testing,” Computer Security Resource Center (CSRC). Diakses: 8 Juli 2025. [Daring]. Tersedia pada: https://csrc.nist.gov/glossary/term/penetration_testing/
- [16] G. M. Khan Tasmiha, “Apa itu Common Vulnerabilities and Exposures (CVE)?” Diakses: 10 Juli 2025. [Daring]. Tersedia pada: <https://www.ibm.com/id-id/think/topics/cve>
- [17] The MITRE Corporation, “CVE Record Lifecycle ,” CVE - Common Vulnerabilities and Exposures. Diakses: 10 Juli 2025. [Daring]. Tersedia pada: <https://www.cve.org/About/Process#CVERecordLifecycle>
- [18] Penetration Testing Execution Standard (PTES), “Technical Report Guide,” Penetration Testing Execution Standard. Diakses: 11 Juli 2025. [Daring]. Tersedia pada: <https://www.pentesting.org/technical-report-guide/>
- [19] Gandhi Krishna dan V Patel Pritibala, “Python: An Inclusive Review of Its

- User-Friendly Nature and Applications,” *International Research Journal on Advanced Engineering and Management (IRJAEM)*, vol. 3, no. 05, hlm. 1872–1875, Mei 2025, doi: 10.47392/irjaem.2025.0293.
- [20] “Sequence Labeling for Part of Speech and Named Entities Part of Speech Tagging.”
 - [21] E. Aghaei, X. Niu, W. Shadid, dan E. Al-Shaer, “SecureBERT: A Domain-Specific Language Model for Cybersecurity,” Okt 2022, [Daring]. Tersedia pada: <http://arxiv.org/abs/2204.02685>
 - [22] H. Xie, Z. Tan, dan X. Lv, “Application of Artificial Intelligence in Financial Risk Management in a Company,” dalam *ACM International Conference Proceeding Series*, Association for Computing Machinery, Des 2024, hlm. 349–354. doi: 10.1145/1122445.1122456.
 - [23] S. B. A. B. S. K. E. B. Ates, “Secure-AI: Artificial Intelligence Driven Security Assessment Methodology for Penetration Testing,” dalam *2024 IEEE International Conference on Big Data (Big Data)*, Sorrento, Italy: IEEE, 2024, hlm. 1084–1093. doi: 10.1109/BigData59063.2024.10698605.
 - [24] B. Chen, Z. Zhang, N. Langrené, dan S. Zhu, “Unleashing the potential of prompt engineering for large language models,” Mei 2025, doi: 10.1016/j.patter.2025.101260.
 - [25] G. Perrone dan S. Pietro Romano, “Prompt Engineering as Code (PEaC): an approach for building modular, reusable, and portable prompts,” dalam *2024 2nd International Conference on Foundation and Large Language Models, FLLM 2024*, Institute of Electrical and Electronics Engineers Inc., 2024, hlm. 289–294. doi: 10.1109/FLLM63129.2024.10852434.
 - [26] P. Liu *dkk.*, “A Survey on Open Information Extraction from Rule-based Model to Large Language Model,” Okt 2024, [Daring]. Tersedia pada: <http://arxiv.org/abs/2208.08690>
 - [27] D. Xu *dkk.*, “Large Language Models for Generative Information Extraction: A Survey,” Okt 2024, [Daring]. Tersedia pada: <http://arxiv.org/abs/2312.17617>
 - [28] H. Zhang, P. S. Yu, dan J. Zhang, “A Systematic Survey of Text

Summarization: From Statistical Methods to Large Language Models,” Jun

2024, [Daring]. Tersedia pada: <http://arxiv.org/abs/2406.11289>

- [29] Jagtap Vandana, Parlewar Pallavi, Dhande Sheetal, Langhe Anagha, Choudhary Harsh, dan Mishra Ashutosh, “Advancements in Text Summarization Through Machine Learning: A Comprehensive Survey and Analysis,” 2024.
- [30] H. Shakil, A. Farooq, dan J. Kalita, “Abstractive Text Summarization: State of the Art, Challenges, and Improvements,” Sep 2024, doi: 10.1016/j.neucom.2024.128255.