DAFTAR PUSTAKA

[1] ITU, *Global Cybersecurity Index 2020*. International Telecommunication Union, 2020. [Online]. Available: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

[2] F. Pratiwi, "BSSN Catat 370,02 Juta Serangan Siber ke Indonesia pada 2022 - Dataindonesia.id," 2023. https://dataindonesia.id/internet/detail/bssn-catat-37002-juta-serangan-siber-ke-indonesia-pada-2022 (accessed Jun. 14, 2024).

[3] BSSN, "Lanskap Keamanan Siber Indonesia," no. 70, 2023, [Online]. Available: https://www.bssn.go.id/wp-content/uploads/2024/03/Lanskap-Keamanan-Siber-Indonesia-2023.pdf

[4] Firda, S. Putri, Y. B. Utomo, and H. Kurniadi, "Analisa Celah Keamanan Pada Website Pemerintah Kabupaten Kediri Menggunakan Metode Penetration Testing Melalui Kali Linux," *Pros. SEMNAS INOTEK (Seminar Nas. Inov. Teknol.*, vol. 7, no. 1, pp. 52–59, 2023, [Online]. Available: https://proceeding.unpkediri.ac.id/index.php/inotek/article/view/3411

[5] U. S. D. of the Interior, "Penetration Testing | U.S. Department of the Interior," 2023. https://www.doi.gov/ocio/customers/penetration-testing (accessed Mar. 07, 2024).

[6] D. F. Priambodo, A. D. Rifansyah, and M. Hasbi, "Penetration Testing Web XYZ Berdasarkan OWASP Risk Rating," *Teknika*, vol. 12, no. 1, pp. 33–46, 2023, doi: 10.34148/teknika.v12i1.571.

[7] B. E. Strom, D. P. Miller, K. C. Nickels, A. G. Pennington, and C. B. Thomas, "MITRE ATT & CK ™ : Design and Philosophy Authors :," no. July, p. 37, 2018.

[8] T. Moore, "The NIST Cybersecurity," p. 32, 2024, [Online]. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[9] N. Teodoro, L. Gonçalves, and C. Serrão, "NIST cybersecurity framework compliance: A generic model for dynamic assessment and predictive requirements," *Proc. - 14th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. Trust. 2015*, vol. 1, pp. 418–425, 2015, doi: 10.1109/Trustcom.2015.402.

[10] G. Culot, G. Nassimbeni, M. Podrecca, and M. Sartor, "The ISO/IEC 27001 information security management standard: literature review and theory-based

research agenda," *TQM J.*, vol. 33, no. 7, pp. 76–105, 2021, doi: 10.1108/TQM-09-2020-0202.

[11] A. Kusnandar, "Evaluasi Keamanan Sistem Informasi Menggunakan Fuzzy FMEA Berbasis Framework ISO/IEC 27001:2013 untuk Meningkatkan Keamanan Informasi," *J. Sist. Inf. Bisnis*, vol. 14, no. 2, pp. 181–190, 2024, doi: 10.21456/vol14iss2pp181-190.

[12] Y. Armando and R. Rosalina, "Penetration Testing Tangerang City Web Application With Implementing OWASP Top 10 Web Security Risks Framework," *JISA(Jurnal Inform. dan Sains)*, vol. 6, no. 2, pp. 105–109, 2023, doi: 10.31326/jisa.v6i2.1656.

[13] M. Lanni and A. Kurniawan, "Boosting Cyber Risk Assessment in Government Entities through Combined NIST and MITRE ATT&CK Threat Modeling," *J. Syst. Manag. Sci.*, vol. 14, no. 6, pp. 283–299, 2024, doi: 10.33168/jsms.2024.0618.

[14] G. Kusuma, "Implementasi Owasp Zap Untuk Pengujian Keamanan Sistem Informasi Akademik," *J. Teknol. Inf. J. Keilmuan dan Apl. Bid. Tek. Inform.*, vol. 16, no. 2, pp. 178–186, 2022, doi: 10.47111/jti.v16i2.3995.

[15] Y. Jo, O. Choi, J. You, Y. Cha, and D. H. Lee, "Cyberattack Models for Ship Equipment Based on the MITRE ATT&CK Framework," *Sensors*, vol. 22, no. 5, pp. 1–18, 2022, doi: 10.3390/s22051860.

[16] M. Albahar, D. Alansari, and A. Jurcut, "An Empirical Comparison of Pen-Testing Tools for Detecting Web App Vulnerabilities," *Electron.*, vol. 11, no. 19, pp. 1–25, 2022, doi: 10.3390/electronics11192991.

[17] M. F. F. Ikhsan, E. I. Alwi, and T. Hasanuddin, "Website vulnerability analysis PT . Sadikun Niaga Mas Raya Uses the Owasp Penetration Testing Method," *Int. J. Multidiscip. Res. Growth Eval.*, vol. 05, no. 01, pp. 418–425, 2024.

[18] "Dinas Sosial Kota Surabaya," 2021. https://dinassosial.surabaya.go.id/ (accessed Jun. 14, 2024).

[19] "Peraturan Walikota PERWALI Nomor 75 Tahun 2021 tentang Kedudukan, Susunan Organisasi, Uraian Tugas dan Fungsi Serta Tata Kerja Dinas Sosial Kota Surabaya," Sep. 21, 2021. https://jdih.surabaya.go.id/peraturan/3961 (accessed Jun. 14, 2024).

[20] E. A. Altulaihan, A. Alismail, and M. Frikha, "A Survey on Web Application

Penetration Testing," *Electron.*, vol. 12, no. 5, 2023, doi: 10.3390/electronics12051229.

[21] K. Božić, N. Penevski, and S. Adamović, "Penetration Testing and Vulnerability Assessment: Introduction, Phases, Tools and Methods," pp. 229–234, 2019, doi: 10.15308/sinteza-2019-229-234.

[22] P. K. Ayuningtyas, D. Atmodjo WP, and P. Rachmadi, "Performance And Functional Testing With The Black Box Testing Method," *Int. J. Progress. Sci. Technol.*, vol. 39, no. 2, p. 212, 2023, doi: 10.52155/ijpsat.v39.2.5471.

[23] S. Nidhra, "Black Box and White Box Testing Techniques - A Literature Review," *Int. J. Embed. Syst. Appl.*, vol. 2, no. 2, pp. 29–50, 2012, doi: 10.5121/ijesa.2012.2204.

[24] C. Kalpana, "A Research Paper on White Box Testing," *Data Anal. Artif. Intell.*, vol. 2, no. 6, pp. 40–43, 2022, doi: 10.46632/daai/2/6/8.

[25] L. Nguyen, A. Simmons, H.-A. Tran, and T. Tran, "Security Testing of a Smart Home Management System using Formal Method and Gray-box Testing," pp. 0–25, 2023.

[26] S. Acharya and V. Pandya, "Bridge between Black Box and White Box - Gray Box Testing Technique," *Int. J. Electron. Comput. Sci. Eng.*, vol. 2, no. 1, pp. 175–85, 2013, [Online]. Available: http://www.estdl.org/wp-content/uploads/2013/03/Volume-2Number-1PP-175-185.pdf

[27] I. Odun-Ayo *et al.*, "Evaluating Common Reconnaissance Tools and Techniques for Information Gathering," *J. Comput. Sci.*, vol. 18, no. 2, pp. 103–115, 2022, doi: 10.3844/jcssp.2022.103.115.

[28] M. F. Safitra, M. Lubis, and A. Widjajarto, "Security Vulnerability Analysis using Penetration Testing Execution Standard (PTES): Case Study of Government's Website," *ACM Int. Conf. Proceeding Ser.*, pp. 139–145, 2023, doi: 10.1145/3592307.3592329.

[29] Y. Khera, D. Kumar, S. Sujay, and N. Garg, "Analysis and Impact of Vulnerability Assessment and Penetration Testing," *Proc. Int. Conf. Mach. Learn. Big Data, Cloud Parallel Comput. Trends, Prespectives Prospect. Com. 2019*, no. May, pp. 525–530, 2019, doi: 10.1109/COMITCon.2019.8862224.

[30] F. Heiding, E. Süren, J. Olegård, and R. Lagerström, "Penetration testing of connected households," *Comput. Secur.*, vol. 126, 2023, doi:

10.1016/j.cose.2022.103067.

[31] M. C. Osazuwa, O. Mitchell, and C. Osazuwa, “Confidentiality, Integrity, and Availability in Network Systems: A Review of Related Literature,” *Int. J. Innov. Sci. Res. Technol.*, vol. 8, no. 12, 2023.

[32] A. S. Sikder, “Cybersecurity Framework for Ensuring Confidentiality, Integrity, and Availability of University Management Systems in Bangladesh.: Cybersecurity framework on UMS in Bangladesh,” *Int. J. Imminent Sci. \& Technol.*, vol. 1, no. 1, pp. 17–39, 2023, doi: 10.13140/RG.2.2.15091.30241.

[33] A. Haddad, N. Aaraj, P. Nakov, and S. F. Mare, “Automated Mapping of CVE Vulnerability Records to MITRE CWE Weaknesses,” 2023, [Online]. Available: http://arxiv.org/abs/2304.11130

[34] M. Saletta and C. Ferretti, “A Neural Embedding for Source Code: Security Analysis and CWE Lists,” *Proc. - IEEE 18th Int. Conf. Dependable, Auton. Secur. Comput. IEEE 18th Int. Conf. Pervasive Intell. Comput. IEEE 6th Int. Conf. Cloud Big Data Comput. IEEE 5th Cybe*, pp. 523–530, 2020, doi: 10.1109/DASC-PICom-CBDCom-CyberSciTech49142.2020.00095.

[35] N. Vugdelija, “Use of ‘owasp top 10’ in we b application security,” pp. 25–30, 2020.

[36] “OWASP Top 10:2021.” https://owasp.org/Top10/ (accessed Jun. 14, 2024).

[37] “MITRE ATT&CK®,” 2024. https://attack.mitre.org/ (accessed Jun. 14, 2024).

[38] S. Kashman, “Google Dorking or Legal Hacking: From the Cia Google Dorking or Legal Hacking: From the Cia Compromise To Your Cameras At Home, We Are Not As Compromise To Your Cameras At Home, We Are Not As Safe As We Think Safe As We Think,” *Technol. Arts Washingt. J. Law*, vol. 18, no. February, pp. 1–2, 2023, [Online]. Available: https://digitalcommons.law.uw.edu/wjltahttps://digitalcommons.law.uw.edu/wjlta/vol18/iss2/1Electroniccopyavailableat:https://ssrn.com/abstract=4369984

[39] J. L. Wan, “Key Characteristics and Conceptual Architecture of Mozilla Firefox,” no. June, 2020.

[40] “Wappalyzer.” https://www.wappalyzer.com/ (accessed Jun. 14, 2024).

[41] S. K. G. and A. Singh, “Hands-On Guide to Virtual Box,” pp. 194–207, 2017, doi: 10.4018/978-1-5225-2785-5.ch008.

[42] P. Surarapu, “An Overview of Kali Linux : Empowering Ethical Hackers with

Unparalleled FMDB Transactions on Sustainable Technoprise Letters An Overview of Kali Linux : Empowering Ethical Hackers with Unparalleled Features," no. December, 2023.

[43] "Nmap: the Network Mapper - Free Security Scanner." https://nmap.org/ (accessed Jun. 14, 2024).

[44] "Nessus Vulnerability Scanner." https://www.tenable.com/products/nessus (accessed Jun. 14, 2024).

[45] "sqlmap: automatic SQL injection and database takeover tool." https://sqlmap.org/ (accessed Jun. 14, 2024).

[46] M. Mada, "Install Bettercap di Kali Linux 2020.x | by Muhammad Mada | MADATECH | Medium," Jan. 21, 2021. https://medium.com/madatech/install-bettercap-di-kali-linux-20-x-fa2600ff381f (accessed Nov. 06, 2024).

[47] "ZAP." https://www.zaproxy.org/ (accessed Jun. 14, 2024).

[48] C. Mainka, V. Mladenov, T. Guenther, and J. Schwenk, "Automatic recognition, processing and attacking of single sign-on protocols with burp suite," *Lect. Notes Informatics (LNI), Proc. - Ser. Gesellschaft fur Inform.*, vol. 251, pp. 117–131, 2015.

[49] "NVD - CVE-2019-8331." https://nvd.nist.gov/vuln/detail/CVE-2019-8331 (accessed Nov. 03, 2024).