Daftar Pustaka

[1] J.-P. A. Yaacoub, H. N. Noura, O. Salman, and A. Chehab, "Ethical hacking for IoT: Security issues, challenges, solutions and recommendations," *Internet of Things and Cyber-Physical Systems*, vol. 3, pp. 280–308, Apr. 2023. [Online]. Available: https://doi.org/10.1016/j.iotcps.2023.04.002

[2] F. Chen, J. Zhu, Y. Huo, and D. Fan, "A review on the study on MQTT security challenge," in *2020 IEEE International Conference on Smart Cloud (SmartCloud)*, 2020, pp. 128-133. doi: 10.1109/SmartCloud49737.2020.00032.

[3] A. J. Hintaw, S. Manickam, M. F. Aboalmaaly, and S. Karuppayah, "MQTT vulnerabilities, attack vectors and solutions in the Internet of Things (IoT)," *IETE Journal of Research*, pp. 1-9, May 2021. doi: 10.1080/03772063.2021.1912651

[4] M. Denis, C. Zena, and T. Hayajneh, "Penetration testing: Concepts, attack methods, and defense strategies," *New York Institute of Technology*, 2016.

[5] C. Tagliarro, M. Komsic, A. Continella, K. Borgolte, and M. Lindorfer, "Large-scale security analysis of real-world backend deployments speaking IoT-focused protocols," *arXiv*, 2024. doi: 10.48550/arXiv.2405.09662.

[6] G. Chu and A. Lisitsa, "Penetration Testing for Internet of Things and Its Automation," 2018 IEEE Access 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS), Exeter, UK, 2018, pp. 1479-1484, doi: 10.1109/HPCC/SmartCity/DSS.2018.00244.

[7] B. Mishra dan A. Kertesz, "The Use of MQTT in M2M and IoT Systems: A Survey," *IEEE Access*, vol. 8, pp. 201071-201082, Nov. 2020. DOI: 10.1109/ACCESS.2020.3035849

[8] IBM X-Force, "Stealthy WailingCrab malware misuses MQTT messaging protocol," *Security Intelligence*, Oct. 25, 2024. [Online]. Available: https://securityintelligence.com/x-force/wailingcrab-malware-misues-mqtt-messaging-protocol/. [Accessed: Oct. 25, 2024].

[9] B. D. Davis, J. C. Mason, and M. Anwar, "Vulnerability studies and security postures of IoT devices: A smart home case study," *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 10102-10109, Oct. 2020, doi: 10.1109/JIOT.2020.2983983.

[10] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A Survey on Security and Privacy Issues in Internet-of-Things," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1250-1258, Oct. 2017, doi: 10.1109/JIOT.2017.2694844.

[11] R. A. Suari and I. M. Sarjana, "Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia," *Jurnal Analisis Hukum (JAH)*, vol. 6, no. 1, pp. 132-146, Apr. 2023, doi: 10.38043/jah.v6i1.4484.

[12] M. Aldabbas, X. Xie, B. Teufel, and S. Teufel, "Future security challenges for smart societies: Overview from technical and societal perspectives," in *2020 8th International Conference on Smart Grid and Clean Energy Technologies (ICSGCE)*, 2020, pp. 103–111. [Online]. Available: https://doi.org/10.1109/ICSGCE49163.2020.9284894

[13] IBM, "Escalating Data Breach Disruption Pushes Costs to New Highs," IBM Newsroom, 2024. [Online]. Available: https://newsroom.ibm.com/escalating-data-breach-2024. [Accessed: Oct. 22, 2024].

[14] IBM, "Cost of a Data Breach Report 2024," IBM Security, 2024. [Online]. Available: https://www.ibm.com/security/data-breach. [Accessed: Oct. 22, 2024].

[15] G. D. Singh, *The Ultimate Kali Linux Book: Perform Advanced Penetration Testing Using Nmap, Metasploit, Aircrack-ng, and Empire*, Jerman: Packt Publishing, 2022.

[16] "Network Mapper," Nmap. [Online]. Available: https://nmap.org/. [Accessed: Oct. 19, 2024].

[17] R. Asaad, "Penetration Testing: Wireless Network Attacks Method on Kali Linux OS," *Academic Journal of Nawroz University*, vol. 10, no. 1, pp. 7, 2021. doi: 10.25007/ajnu.v10n1a998.

[18] D. Abeles and M. Zioni, "MQTT-PWN, IoT exploitation & recon framework," [Online]. Available: https://mqtt-pwn.readthedocs.io/en/latest/index.html. [Accessed: Oct. 19, 2024].

[19] A. Palmieri, P. Prem, S. Ranise, U. Morelli and T. Ahmad, "MQTTSA: A Tool for Automatically Assisting the Secure Deployments of MQTT Brokers," 2019 IEEE World Congress on Services (SERVICES), Milan, Italy, 2019, pp. 47-53, doi: 10.1109/SERVICES.2019.00023.

[20] souravbaghz, "MQTTack," GitHub repository, 2023. [Online]. Avaible: https://github.com/souravbaghz/MQTTack

[21] Syaiful Andy, Budi Rahardjo, and Bagus Hanindhito, "Attack Scenarios and Security Analysis of MQTT Communication Protocol in IoT System," *Proceedings of the EECSI 2017*, Yogyakarta, Indonesia, Sep. 2017, pp. 600–601, doi: 10.1109/EECSI.2017.8257317.

[22] S. Shah and M. Dave, "Man-in-the-Middle Attacks on MQTT based IoT networks," Master's Thesis, Missouri University of Science and Technology, Rolla, Missouri, USA, 2019. [Online]. Available: https://scholarsmine.mst.edu/masters_theses/8102

[23] S. A. Altayaran and W. Elmedany, "Integrating Web Application Security Penetration Testing into the Software Development Life Cycle: A Systematic Literature Review," *2021 International Conference on Data Analytics for Business and Industry (ICDABI)*, Sakheer, Bahrain, 2021, pp. 671-676, doi: 10.1109/ICDABI53623.2021.9655950.

[24] ISO/IEC, "Information technology — Message Queuing Telemetry Transport (MQTT) v3.1.1," ISO/IEC 20922:2016(E), International Standard, Jun. 2016

[25] J. Voas, "Networks of 'Things'," *NIST Special Publication 800-183*, U.S. Department of Commerce, National Institute of Standards and Technology, July 2016. [Online]. Available: http://dx.doi.org/10.6028/NIST.SP.800-183:contentReference[oaicite:0]{index=0}.

[26] OWASP Toronto Chapter, "OWASP IoT Top 10 - Introduction and Root Causes," [PDF presentation], Dec. 11, 2019. Available: https://owasp.org/www-chapter-toronto/assets/slides/2019-12-11-OWASP-IoT-Top-10---Introduction-and-Root-Causes.pdf.

[27] G. Van Rossum and F. L. Drake, Python 3 Reference Manual. CreateSpace, 2009.

[28] D. Flanagan, JavaScript: The Definitive Guide, 7th ed. O'Reilly Media, 2020.

[29] A. A. A. Donovan and B. W. Kernighan, The Go Programming Language. Addison-Wesley Professional, 2015.

[30] S. Meyers, Effective Modern C++: 42 Specific Ways to Improve Your Use of C++11 and C++14. O'Reilly Media, 2014.

[31] C. Anderson, "Docker [software engineering]," IEEE Software, 2015. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7093032/

[32] Amazon Web Services, "Docker on AWS," AWS Documentation. [Online]. Available: https://aws.amazon.com/docker/

[33] M. Muslihudin and Helmiyanto, "Jurnal simada," Jurnal Sistem Informasi Manajemen Basis Data, vol. 03, no. 01, p. 68, 2020.

[34] I. Alkhwaja *et al.*, "Password Cracking with Brute Force Algorithm and Dictionary Attack Using Parallel Programming," *Applied Sciences*, vol. 13, no. 10, p. 5979, May 2023. [Online]. Available: https://doi.org/10.3390/app13105979. [Accessed: Dec. 28, 2024].

[35] Wang, H., Xu, L., & Gu, G. (2015). *FloodGuard: A DoS Attack Prevention Extension in Software-Defined Networks. 2015 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks.* doi:10.1109/dsn.2015.27

[36] A. F. Gentile, D. Macrì, D. L. Carnì, and E. Greco, "A Network Performance Analysis of MQTT Security Protocols with Constrained Hardware in the Dark Net for DMS," *Applied Sciences*, vol. 14, no. 18, p. 8501, Sep. 2024. [Online]. Available: https://doi.org/10.3390/app14188501. [Accessed: Dec. 28, 2024].

[37] K. 'Afiifah, Z. F. Azzahra, and A. D. Anggoro, "Analisis Teknik Entity-Relationship Diagram dalam Perancangan Database: Sebuah Literature Review," *Jurnal INTECH*, vol. 3, no. 1, pp. 8–11, Mei 2022. [Online]. Available:http://journal.unbara.ac.id/index.php/INTECH.

[38] S. Liao, C. Zhou, Y. Zhao, Z. Zhang, C. Zhang, Y. Gao, and G. Zhong, "A comprehensive detection approach of Nmap: Principles, rules and experiments," in *Proc. 2020 Int. Conf. Cyber-Enabled Distributed Comput. Knowl. Discovery (CyberC)*, Wuhan, China, 2020, pp. 64–71, doi: 10.1109/CYBERC49757.2020.00020.

[39] M. Moharir, "Scapy Scripting to Automate Testing of Networking Middleboxes," *Advances in Science, Technology and Engineering Systems Journal*, vol. 5, no. 2, pp. 293–298, 2020. [Online]. Available: https://www.astesj.com/publications/ASTESJ_050238.pdf

[40] The Qt Company, "Qt for Python," *Qt Documentation*, 2025. [Online]. Available: https://www.qt.io/qt-for-python

[41] D. Kant, A. Johannsen, and R. Creutzburg, "Analysis of IoT security risks based on the exposure of the MQTT protocol," *Electronic Imaging*, vol. 2021, no. 11, pp. 267-1–267-8, Jan. 2021. [Online]. Available: https://www.researchgate.net/publication/354766164_Analysis_of_IoT_Security_Risks_based_on_the_exposure_of_the_MQTT_Protocol

[42] K. Salah, M. H. Alharthi, and R. Boutaba, “Performance evaluation and testing of MQTT brokers: A review,” *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2222–2235, 2021, doi: 10.1109/JIOT.2020.3023456.

[43] S. Pawar, N. Panigrahi, J. A. P., M. Lokhande, D. Godse, dan D. B. Jadhav, "Evaluation of Delay Parameter of MQTT Protocol," *International Journal of Engineering Trends and Technology*, vol. 71, no. 3, pp. 227–235, 2023. [Online]. Tersedia: https://doi.org/10.14445/22315381/IJETT-V71I3P223

[44] D. Richard Hipp, “SQLite Documentation: Datatypes In SQLite Version 3,” SQLite.org, 2024. [Online]. Available: https://www.sqlite.org/datatype3.html

[45] “Report On Coding & Testing in Software Engineering,” ResearchGate, 2023. [Online]. Available: https://doi.org/10.13140/RG.2.2.33051.44321

[46] A. Jamil, M. Arif, N. S. A. Abubakar, and A. Ahmad, “Software Testing Techniques: A Literature Review,” in *Proc. 2016 6th Int. Conf. on Information and Communication Technology for The Muslim World (ICT4M)*, Nov. 2016, pp. 177–182, doi: 10.1109/ICT4M.2016.045

[47] D. I. Pirdaus and R. A. Hidayana, “Analysis Testing Black Box and White Box on Application To-Do List Based Web,” *Int. J. Math. Stat. Comput.*, vol. 2, no. 2, pp. 68–75, 2024.

[48] T. D. Capote, “A comparative study of black box and white box testing techniques in modern software development,” *Frontiers in Engineering and Technology*, vol. 5, no. 1, pp. 1–7, Jan.–Jun. 2024. [Online]. Available: https://iaeme.com/MasterAdmin/Journal_uploads/FET/VOLUME_5_ISSUE_2/FET_05_01_001.pdf

[49] Abdeen, W., Chen, X. & Unterkalmsteiner, M. An approach for performance requirements verification and test environments generation. *Requirements Eng* 28, 117–144 (2023). https://doi.org/10.1007/s00766-022-00379-3

[50] J. C. S. J. Pan, J. M. F. de la Hoz, M. D. R-Moreno, dan A. F. G. Skarmeta, “Performance analysis of IoT application layer protocols on constrained devices,” dalam *Proc. 14th Int. Conf. on Future Networks and Communications (FNC)*, 2019, hlm. 355-362

[51] H. K. N. Leung and P. W. L. Wong, "A study of user acceptance tests," *Software Quality Journal*, vol. 6, no. 2, pp. 137–149, Jun. 1997. doi: 10.1023/A:1018503800709.

[52] S. U. A. Laghari, W. Li, S. Manickam, P. Nanda, dan A. Khallel, "Securing MQTT Ecosystem: Exploring Vulnerabilities, Mitigations, and Future Trajectories," *IEEE Access*, vol. 11, hlm. 143196-143215, 2023, doi: 10.1109/ACCESS.2023.3342885.

[53] PurpleSec, "White Box Penetration Testing: The Assumed Breach," PurpleSec, 2023. [Online]. Tersedia: https://purplesec.us/learn/white-box-penetration-testing/.

[54] J. Straub, "Modeling Attack, Defense and Threat Trees and the Cyber Kill Chain, ATTCK and STRIDE Frameworks as Blackboard Architecture Networks," in Proc. 2020 IEEE Int. Conf. on Smart Cloud (SmartCloud), Nov. 2020, pp. 148–153, doi: 10.1109/SmartCloud49737.2020.00035.

[55] Kartono, H., Harwahyu, R., "Pemodelan Ancaman STRIDE/DREAD pada Sistem Diseminasi Terintegrasi," Smart Comp: Jurnalnya Orang Pintar Komputer, vol. 12, no. 4, pp. 1060–1071, Okt. 2023, doi: 10.30591/smartcomp.v12i4.5698.