DAFTAR PUSTAKA

[1] S. Madakam, R. Ramaswamy, and S. Tri*path*i, "*Internet of Things* (IoT): A literature review," J. Comput. Commun., vol. 3, no. 5, pp. 164–173, 2015.

[2] F. Susanto, N. K. Prasiani, and P. Darmawan, "Implementasi *Internet of Things* dalam kehidupan sehari-hari," J. Imagine, vol. 2, no. 1, pp. 35–40, 2022.

[3] E. D. Meutia, "*Internet of Things*-keamanan dan privasi," in Semin. Nas. dan Expo Tek. Elektro, vol. 1, no. 1, 2015.

[4] W. Najib and S. Sulistyo, "Tinjauan ancaman dan solusi keamanan pada teknologi *Internet of Things*," J. Nas. Tek. Elektro dan Teknol. Inf., vol. 9, no. 4, pp. 375–384, 2020.

[5] Flipper *Device*s Inc., "Flipper Zero: Portable multi-to*ol device for pentest*ers and geeks." [Online]. Available: https://flipperzero.one. [Accessed: Nov. 24, 2024].

[6] S. Shah and B. M. Mehtre, "An overview of vulnerability assessment and *penetration Testing* techniques," J. Comput. Virol. Hacking Tech., vol. 11, no. 1, pp. 27–49, Nov. 2016.

[7] M. C. Ghanem and T. M. Chen, "Rein*for* cement learning *for* efficient network *penetration Testing*," In*formati*on, vol. 11, no. 1, p. 6, 2019.

[8] R. M. S. Awalsyah, P. S. Harahap, and M. Dono, "Implementasi caesar cipher dalam mengenkripsikan pesan pada serangan man in the middle attack," JOCITIS-J. Sci. Inf. Robot., vol. 1, no. 1, pp. 64–72, 2023.

[9] EmenstaNougat, "ESP32-BlueJammer," GitHub, 2018. [Online]. Available: https://github.com/EmenstaNougat/ESP32-BlueJammer. [Accessed: Dec. 20, 2024].

[10] Wireshark *Found*ation, "Extcap *capture interface*," Wireshark Documentation. [Online]. Available: https://www.wireshark.org/docs/wsdg_html_chunked/Ch*Capture*Extcap.html. [Accessed: Jun. 17, 2024].

[11] S. Cass, "A hacker's delight: You'll either love or hate the Flipper Zero," IEEE Spectr., vol. 60, no. 5, 2023.

[12] D. Cauquil, "Btlejack: *Bluetooth low energy* swiss-army knife," GitHub, 2018. [Online]. Available: https://github.com/virtualabs/btlejack. [Accessed: Dec. 20, 2024].

[13] R. Pava, R. Martin, and S. Mishra, “Unveiling exploitation potential: a comparative analysis of Flipper Zero and rubber ducky,” Issues Inf. Syst., vol. 25, no. 2, pp. 84–95, 2024.

[14] W. C. Wang, “Legal, policy, and compliance issues in using AI *for* security: Using Taiwan’s *cybersecurity* management act and *penetration Testing* as examples,” in Unknown Conference, May 2024, pp. 161–176.

[15] Republik Indonesia, Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Jakarta: Sekretariat Negara, 2022.

[16] Republik Indonesia, Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Jakarta: Sekretariat Negara, 2008.

[17] *ControlPath*s, “Hackbat,” GitHub, Oct. 2024. [Online]. Available: https://github.com/*controlpath*s/Hackbat.

[18] V. Hassija, V. Chamola, and V. Saxena, “A survey on IoT security: Application areas, security threats, and solution architectures,” IEEE Internet Things J., 2023.

[19] *ControlPath*s, “The Hackbat: *Open-source* hacking to*ols*.” [Online]. Available: https://theHackbat.com/. [Accessed: Oct. 25, 2024].

[20] C. Ikezuruora, “Beyond headlines: Case study- The Equifax data breach and lessons learned,” PrivacyEnd, Feb. 2024. [Online]. Available: https://www.privacyend.com/case-study-equifax-data-breach-lessons-learned/.

[21] Y. Kristiyanto and E. Ernastuti, “Analysis of *deauth*entication attack on IEEE 802.11 connectivity based on IoT techno*log*y using *External* penetration test,” CommIT (Commun. Inf. Technol.) J., vol. 14, no. 1, pp. 45–51, 2020. DOI: 10.21512/commit.v14i1.6337.

[22] Republik Indonesia, Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Lembaran Negara Republik Indonesia Tahun 2022 Nomor 179, Jakarta, 2022.

[23] Republik Indonesia, Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Jakarta: Sekretariat Negara, 2008.

[24] Flipper *Device*s Inc., “Flipper Zero: Portable multi-to*ol device for pentest*ers and geeks.” [Online]. Available: https://flipperzero.one/. [Accessed: Nov. 24, 2024].

[25] Flipper *Device*s Inc., “Flipper Zero: Portable multi-to*ol device for pentest*ers and geeks.” [Online]. Available: https://flipperzero.one. [Accessed: Oct. 25, 2024].

[26] The OWASP *Found*ation, “OWASP IoT security *Testing* guide,” Ver. 2.0, 2023. [Online]. Available: https://owasp.org/www-project-iot-security-*Testing*-guide.

[27] A. Gupta and Attify, “IoT *pentesting* guide.” [Online]. Available: https://www.iot*pentesting*guide.com/. [Accessed: Nov. 24, 2024].

[28] A. Gupta and Attify, “IoT *pentesting* guide.” [Online]. Available: https://www.iot*pentesting*guide.com/.

[29] A. Shintani, “The design, *Testing*, and analysis of a constant jammer *for* the *Bluetooth Low Energy* (BLE) wireless communication protocol,” M.S. thesis, Dept. Electr. Eng., *California* Polytechnic State Univ., San Luis Obispo, CA, USA, Jun. 2020. [Online]. Available: https://doi.org/10.15368/theses.2020.70.

[30] P. Syverson, “A taxonomy of replay attacks [cryptographic protocols],” in Proc. Comput. Secur. *Found*. Workshop VII, Franconia, NH, USA, 1994, pp. 187–191. DOI: 10.1109/CSFW.1994.315935.

[31] ikarus23, “Mifare *Classic Tool*,” GitHub. [Online]. Available: https://github.com/ikarus23/Mifare*ClassicTool*. [Accessed: Jun. 17, 2024].

[32] NFCGate Team, “NFCGate,” GitHub. [Online]. Available: https://github.com/nfcgate/nfcgate. [Accessed: Jun. 17, 2024].

[33] U. Gupta, “libnfc,” Salsa Debian. [Online]. Available: https://salsa.debian.org/debian/libnfc. [Accessed: Jun. 17, 2024].

[34] Wireshark *Found*ation, “About Wireshark,” Wireshark. [Online]. Available: https://www.wireshark.org/about.html. [Accessed: Jun. 17, 2024].

[35] S. Margaritelli, “Introduction *to* Bettercap,” Bettercap. [Online]. Available: https://www.bettercap.org/intro/. [Accessed: Jun. 17, 2024].

[36] Air*crack*-ng Team, “Air*crack*-ng,” Air*crack*-ng. [Online]. Available: https://www.air*crack*-ng.org/. [Accessed: Jun. 17, 2024].

[37] Wireshark *Found*ation, “Extcap *capture interface*,” Wireshark Documentation. [Online]. Available:

https://www.wireshark.org/docs/wsdg_html_chunked/Ch*Capture*Extcap.html. [Accessed: Jun. 17, 2024].

[38] D. Cauquil, “Btlejack: *Bluetooth low energy* swiss-army knife,” GitHub, 2018. [Online]. Available: https://github.com/virtualabs/btlejack. [Accessed: Dec. 20, 2024].

[39] EmenstaNougat, “ESP32-BlueJammer,” GitHub, 2018. [Online]. Available: https://github.com/EmenstaNougat/ESP32-BlueJammer. [Accessed: Dec. 20, 2024].