# DAFTAR PUSTAKA

[1] Qrator Labs, "Massive Rise in Application Layer DDoS Attacks Observed in Q2 2025," Qrator Labs Research, Jul. 11, 2025. https://qrator.net/blog/details/q2-2025-ddos-bots-and-bgp-incidents-statistics-and

[2] Woollacott, Emma, "Application layer DDoS attacks are skyrocketing – here's why," IT Pro, 15 July 2025. https://www.itpro.com/security/cyber-attacks/application-layer-ddos-attacks-are-skyrocketing-heres-why

[3] Neal, Zachary, dan Kewei Sha, "Analysis of Evil Twin, Deauthentication, and Disassociation Attacks on Wi-Fi Cameras," *Proceedings of the 32nd International Conference on Computer Communications and Networks (ICCCN 2023),* Jul. 2023. DOI: 10.1109/ICCCN580 (Placeholder1)24.2023.10230183.

[4] Australian Federal Police. 2024. "Man Charged over Creation of 'Evil Twin' Free WiFi Networks to Access Personal Data." *Media Release,* June 28, 2024. https://www.afp.gov.au/news-centre/media-release/man-charged-over-creation-evil-twin-free-wifi-networks-access-personal.

[5] R. Mandasari, "Analisis Metode Fluxion Menggunakan Wi-Fi Deauther untuk Uji Keamanan WPA2 pada Perangkat Router Wireless Totolink N300RT," Skripsi, Program Studi Teknik Informatika, Fakultas Teknik, Universitas Islam Riau, Pekanbaru, 2021.

[6] R. A. Selian, "Analisis Penggunaan Fluxion Portable untuk Menguji Wi-Fi dengan Keamanan WPA/WPA2," Skripsi, Program Studi Pendidikan Teknologi Informasi, Fakultas Tarbiyah dan Keguruan, Universitas Islam Negeri Ar-Raniry, Banda Aceh, 2023.

[7] I. M. Lina dan G. R. Fernandes, "Analisis Pola Social Engineering Menggunakan Teknik WiFi Deauther dan Evil Twin," Jurnal/Artikel Ilmiah, Program Studi Teknik Informatika, Fakultas Teknik dan Ilmu Komputer, Universitas Indraprasta PGRI, 2022.

[8] M. Nurbayazi, A. Zafrullah M., dan A. Zubaidi, "Rancang Bangun Pendeteksi Serangan Deauthentication pada Jaringan WiFi Berbasis ESP8266," *Jurnal Teknologi Informasi, Komputer dan Aplikasinya (JTIKA)*, Sep. 2024.

[9] M. Nurdin, A. Pranandi, U. D. F., Y. Hermawan, dan R. Fadlapi, "Serangan Phising WiFi Menggunakan ESP8266: Replikasi Jaringan untuk Penangkapan Informasi Otentikasi," *HUMANITIS: Jurnal Humaniora, Sosial dan Bisnis*, vol. 2, no. 7, pp. 638–649, Jul. 2024, e-ISSN: 2988-6287.

[10] R. Singh, R. Thakkar, M. Thakkar, U. Rote, S. Patil, dan B. Ingle, "WiFi Deauth and Cloning using ESP8266," in *Proc. 2022 5th International Conference on Advances in Science and Technology (ICAST)*, Sep. 2022, pp. 106–111, doi: 10.1109/ICAST55590.2022.10045021.

[11] M. I. Daulay, "Analisis Perbandingan Keamanan WEP, WPA, WPA2 pada Access Point," Skripsi, Program Studi Teknik Informatika, Fakultas Teknik, Universitas Islam Riau, Pekanbaru, 2019.

[12] Maine Basan dan Kaye Timonera, "Wireless Network Security: WEP, WPA, WPA2 & WPA3 Explained," *eSecurity Planet*, 29 April 2024. https://www.esecurityplanet.com/trends/the-best-security-for-wireless-networks

[13] GeeksforGeeks, "Understanding Deauthentication in Wi-Fi Networks," s*GeeksforGeeks*, Sep. 19, 2024. https://www.geeksforgeeks.org/linux-unix/wi-fi-deauthentication-attack-against-802-11-protocol/

[14] Okta, "Evil Twin Attack: Fake WiFi Access Point Vulnerabilities," *Okta Identity 101*, 29 Aug 2024. [Online]. Available: https://www.okta.com/identity-101/evil-twin-attack/

[15] Alsahlany, A. M., Alfatlawy, Z. H., & Almusawy, A. R., "Experimental Evaluation of Different Penetration Security Levels in Wireless Local Area Network," *ResearchGate*, Feb. 2019. [Online]. Available: https://www.researchgate.net/publication/330982933_Experimental_Evaluati

on_of_Different_Penetration_Security_Levels_in_Wireless_Local_Area_Network

[16] S. Poorana Senthilkumar, C. Kumuthini, & P. Dineshkumar, "A Review of MAC Address Filtering and Spoofing in Windows Operating System," *International Education and Research Journal (IERJ)*, vol. 3, no. 5, May 2017. [Online]. Available: ierj.in/journal/index.php/ierj/article/view/1012

[17] IoTDunia, "ESP8266 WiFi Module Guide (2025) – Features, Specs, Uses," IoTDunia, 25 Apr. 2025. https://iotdunia.com/esp8266-wifi-module/

[18] Nurwenda, S., Irawan, B., & Irzaman, "Analisis Kelakuan Denial-of-Service Attack (DoS Attack) pada Jaringan Komputer dengan Pendekatan pada Level Sekuritas", Jurusan Teknik Informatika, FT, Jl. Dipati Ukur, Bandung; Jurusan Fisika, FMIPA IPB, Jl. Raya Pajajaran, Bogor. [Online]. (Tahun tidak tersedia).

[19] Meilinaeka, "Router: Fungsi, Cara Kerja, dan Perbedaan dengan Modem," IT Telkom University, 9 Jul. 2024. https://it.telkomuniversity.ac.id/router-adalah/

[20] Normunds R. & Serhii T., "RouterOS," MikroTik Help Documentation, Jun. 26, 2025. https://help.mikrotik.com/docs/spaces/ROS/pages/328059/RouterOS

[21] TP-Link, "Chapter 4: Configure the Router in Wireless Router Mode," *TL-WR841N V14 User Guide*, TP-Link, diakses 2 September 2025. https://www.tp-link.com/us/user-guides/tl-wr841n_v14/chapter-4-configure-the-router-in-wireless-router-mode?

[22] Schepers, Domien, Aanjhan Ranganathan, dan Mathy Vanhoef, "On the Robustness of Wi-Fi Deauthentication Countermeasures," *Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '22)*, May 2022, San Antonio, TX, USA. ACM, New York, NY, USA, pp. 245–256. DOI: 10.1145/3507657.3528548.