DAFTAR PUSTAKA

Andris, Z., & Sutresna, J. (2024). Implementasi Peretasan Dan Pengamanan Ssid Pada Jaringan Mikrotik RB941-2ND Dengan Metode Deauther dan Evil Twin. *OKTAL : Jurnal Ilmu Komputer dan Sains*, *3*(09), 2250–2259. https://journal.mediapublikasi.id/index.php/oktal/article/view/3784

Arora, A. (2018). *Preventing wireless deauthentication attacks over 802.11 Networks*. http://arxiv.org/abs/1901.07301

Beagle Security. (2020). *Man-in-the-Middle (MITM) Attack: Types, Techniques and Prevention*. https://beaglesecurity.com/blog/article/man-in-the-middle-attack.html

BleepingComputer. (2024). *Australian charged for 'Evil Twin' WiFi attack on plane*. BleepingComputer. https://www.bleepingcomputer.com/news/security/australian-charged-for-evil-twin-wifi-attack-on-plane/

Boncella, R. J. (2002). Wireless Security: An Overview. *Communications of the Association for Information Systems*, *9*. https://doi.org/10.17705/1cais.00915

Dhineshkaarthi, K., Sundar, S., Vidhyapathi, C. M., & Karthikeyan, B. (2016). *Full duplex bidirectional UART communication between PIC microcontrollers*. *11*, 5876–5880.

Espressif Systems. (2023). *ESP32-WROOM-32E & ESP32-WROOM-32UE Datasheet*. https://www.espressif.com/sites/default/files/documentation/esp32-wroom-32e_esp32-wroom-32ue_datasheet_en.pdf

Espressif Systems. (2026). *ESP32-S3 Series Datasheet*. https://documentation.espressif.com/esp32-s3_datasheet_en.pdf

Ghanem, M. C., & Ratnayake, D. N. (2016). Enhancing WPA2-PSK four-way handshaking after re-authentication to deal with de-authentication followed by *brute-force* attack: A novel re-authentication protocol. *2016 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, CyberSA 2016*, 1–7. https://doi.org/10.1109/CyberSA.2016.7503286

honoki.net. (2015). *How to set up a Wifi captive portal*. https://honoki.net/2015/01/30/how-to-set-up-a-wifi-captive-portal/

Larose, K., Dolson, A. D., & Liu Google, H. (2020). *RFC 8952: Captive portal Architecture* (Nomor 8952). RFC Editor. https://doi.org/10.17487/RFC8952

Lina, I. M., & Fernandes, G. R. (2022). Analisis Pola Sosial Engineering Menggunakan Teknik Wifi Deauther Dan Evil Twin. *JRKT (Jurnal Rekayasa Komputasi Terapan)*, *2*(04). https://doi.org/10.30998/jrkt.v2i04.8185

Mallik, A. (2019). Man-in-the-Middle-Attack: Understanding in Simple Words. *Cyberspace: Jurnal Pendidikan Teknologi Informasi*, *2*(2), 109. https://doi.org/10.22373/cj.v2i2.3453

Mauluddin, E., & Desyani, T. (2024). 5. Jurnal Ilmu Komputer dan Science Implementasi Pengamanan Jaringan Dengan Teknik *Penetration testing* Menggunakan Metode Deauther Dan Evil Twin Pada Wireless Tl-WR840N. *Jurnal Ilmu Komputer dan Science*, *3*(4), 1–15. https://journal.mediapublikasi.id/index.php/oktal

Networkguru.ru. (2022). *Evil Twin attack: Use Cases and Defenses*. https://networkguru.ru/ataka-evil-twin/

Selvarathinam, N. S., Dhar, A. K., & Biswas, S. (2019). *Evil Twin attack* detection using discrete event systems in IEEE 802.11 Wi-Fi networks. *27th Mediterranean Conference on Control and Automation, MED 2019 - Proceedings*, 316–321. https://doi.org/10.1109/MED.2019.8798568

Sepio Cyber. (2021). *Evil Twin attack: What It Is and How It Works*. https://sepiocyber.com/blog/evil-twin-attack/

Setiawan, B., Maulani, M., Putra, Z. P., & Brennaf, M. S. (2025). *Dual*-Interface WiFi Packet Sniffer System using ESP32-CAM with Real-Time PCAP Generation for IoT Network Analysis. *Makara Journal of Technology*, *29*(3). https://doi.org/10.7454/mst.v29i3.1734

Sigit, M., Singasatia, D., & Kurniawan, I. (2024). Pengujian Serangan Evil Twin ESP8266 pada Wireless Networking dengan Metode *Penetration testing*. *Jurnal Ilmiah Sain dan Teknologi*, *2*(11), 193–214. https://jurnal.kolibi.org/index.php/scientica/article/view/2770