

DAFTAR PUSTAKA

- [1] B. Schneier, "The Process of Security," April 2000. [Online]. Available: https://www.schneier.com/essays/archives/2000/04/the_process_of_secur.html. [Accessed 1 May 2021].
- [2] M. Vanhoef and F. Piessens, "Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2," in *Proceedings of the 24th ACM Conference on Computer and Communications Security (CCS)*, New York, USA, Association for Computing Machinery, 2017.
- [3] A. Shanley, "Penetration Testing Frameworks and Methodologies: A Comparison and Evaluation," 2016.
- [4] "Understanding 802.1X Authentication," Huawei, Shenzhen, People's Republic of China, 2019.
- [5] K. Scarfone, M. Souppaya, A. Cody and A. Orebaugh, "Special Publication (SP) 800-115: Technical Guide to Information Security Testing and Assessment," National Institute of Standards and Technology, Gaithersburg, MD, 2008.
- [6] H. M. Adams, "Demo Company Security Assessment Findings Report," 28 May 2019. [Online]. Available: <https://github.com/hmaverickadams/TCM-Security-Sample-Pentest-Report>. [Accessed 17 May 2021].
- [7] "Kondisi Terkini Infrastruktur Jaringan Teknik Elektro," Departemen Teknik Elektro dan Teknologi Informasi, Fakultas Teknik Universitas Gadjah Mada (DTETI FT UGM), Yogyakarta, 2017.
- [8] M. K. Kissi and M. Asante, "Penetration Testing of IEEE 802.1X Port-based Authentication Protocols using Kali Linux Hacking Tools," *International Journal of Computer Applications*, vol. 174, 26 Maret 2021.
- [9] T. Radivilova and H. A. Hassan, "Test for penetration in Wi-Fi network: Attacks on WPA2-PSK and WPA2-enterprise," in *2017 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo)*, Odessa, Ukraine, 2017.
- [10] T. Perković, M. Bugarić, A. Dagelić and M. Čagalj, "On WPA2-Enterprise Privacy in High Education and Science," in *Security and Communication Networks*, Hoboken, NJ, Wiley, 2020.
- [11] B. Caudill, "Four Things Every Penetration Test Report Should Have," 28 December 2017. [Online]. Available: <https://rhinosecuritylabs.com/penetration-testing/four-things-every-penetration-test-repor>. [Accessed 13 June 2021].
- [12] D. Kusumasari, "Status Hukum Pencantuman Disclaimer dalam Situs Internet," HukumOnline.com, 28 February 2011. [Online]. Available: <https://www.hukumonline.com/klinik/detail/ulasan/lt4d5e3dfc6af24/status-hukum-pencantuman-disclaimer-dalam-situs-internet/>. [Accessed 15 June 2021].
- [13] L. Tigar, "Executive Summary: 5 Do's, 5 Don'ts, 5 Examples for Writing Effective Ones," ClearVoice, 24 April 2020. [Online]. Available: <https://www.clearvoice.com/blog/what-is-an-executive-summary/>. [Accessed 16 June 2021].
- [14] "Penetration Test Report," Offensive Security Services, LLC, Cornelius, NC, 2013.
- [15] V. Pillitteri, E. Takamura, N. Goren, A. Regenscheid, K. Dempsey, N. Lefkovitz, C. Enloe, K. Boeckl and J. Boyens, "Special Publication (SP) 800-53 Revision 5: Security and Privacy Controls for Information Systems and Organizations," National Institute of Standards and Technology, Gaithersburg, MD, 2020.
- [16] Forum of Incident Response and Security Teams, "Common Vulnerability Scoring System version 3.1 User Guide," June 2019. [Online]. Available: https://www.first.org/cvss/v3-1/cvss-v31-user-guide_r1.pdf. [Accessed 18 June 2021].
- [17] P. Putman, "The Evil Twin Attack: Safe use of Public Internet," US Cybersecurity Magazine, 17 January 2019. [Online]. Available: <https://www.uscybersecurity.net/evil-twin/>. [Accessed 19 June 2021].
- [18] J. Bellardo and S. Savage, "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions," in *USENIX Security Symposium*, Washington, DC, 2003.
- [19] C. Hosmer, Python Forensics: A Workbench for Inventing and Sharing Digital Forensic Technology, Rockland Town, MA: Syngress Publishing, 2014.
- [20] "All You Need to Know About Packet Sniffers," Tek-Tools Software, 04 May 2020. [Online]. Available: <https://www.tek-tools.com/network/all-about-packet-sniffers>. [Accessed 5 August 2021].
- [21] A. Pradhan and R. Mathew, "Solutions to Vulnerabilities and Threats in Software Defined Networking (SDN)," *Procedia Computer Science*, vol. 171, p. 2585, 2020.



- [22] D. Robb, "Wireshark: Pen Testing Product Overview and Analysis," eSecurity Planet, 01 October 2019. [Online]. Available: <https://www.esecurityplanet.com/products/wireshark/>. [Accessed 05 August 2021].
- [23] M. E. Shacklett, "What is an Attack Vector?," TechTarget, 13 April 2021. [Online]. Available: <https://searchsecurity.techtarget.com/definition/attack-vector>. [Accessed 26 August 2021].
- [24] Cisco Systems, Inc., "PMKID Vulnerability FAQ - WPA/WPA2-PSK and 802.11r," Cisco Meraki, 2020.
- [25] P. Grubbs, "What is EAP-TLS?," SecureW2, 20 January 2021. [Online]. Available: <https://securew2.com/blog/what-is-eap-tls>. [Accessed 04 September 2021].
- [26] J. Ludin, "Public Key Infrastructure: Explained," SecureW2, 30 September 2019. [Online]. Available: <https://securew2.com/blog/public-key-infrastructure-explained>. [Accessed 04 September 2021].