DAFTAR PUSTAKA

[1] 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.

[2] 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.

[3] "Penetration Test Report," Offensive Security Services, LLC, Cornelius, NC, 2013.

[4] 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].

[5] 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].

[6] 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.

[7] A. Shanley, "Penetration Testing Frameworks and Methodologies: A Comparison and Evaluation," 2016.

[8] "Understanding 802.1X Authentication," Huawei, Shenzhen, People's Republic of China, 2019.

[9] "Kondisi Terkini Infrastruktur Jaringan Teknik Elektro," Departemen Teknik Elektro dan Teknologi Informasi, Fakultas Teknik Universitas Gadjah Mada (DTETI FT UGM), Yogyakarta, 2017.

[10] 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.

[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] 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].

[15] 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].

[16] J. Bellardo and S. Savage, "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions," in *USENIX Security Symposium*, Washington, DC, 2003.

[17] S. Almes, "Hostapd Linux Documentation," 21 02 2021. [Online]. Available: https://wireless.wiki.kernel.org/en/users/documentation/hostapd. [Accessed 21 July 2021].

[18] B. Antoniewicz, "HostAPD-WPE Documentation Repository," OpenSecurityResearch, 04 November 2017. [Online]. Available: https://github.com/OpenSecurityResearch/hostapd-wpe. [Accessed 27 July 2021].

[19] "RADIUS (Remote Authentication Dial-In User Service)," TechTarget, June 2007. [Online]. Available: https://searchsecurity.techtarget.com/definition/RADIUS. [Accessed 27 July 2021].

[20] K. Dalbehera, "Understand and Cracking WPA/WPA2 (Enterprise)," 09 August 2018. [Online]. Available: https://teckk2.github.io/wifi%20pentesting/2018/08/09/Cracking-WPA-WPA2-Enterprise.html. [Accessed 31 July 2021].

[21] "Package: libnl-genl-3-dev - Development Library and Headers for libnl-genl-3," [Online]. Available: https://packages.debian.org/sid/libnl-genl-3-dev. [Accessed 31 July 2021].

[22] "Package: libssl-dev - Secure Sockets Layer Toolkit and Development Files," [Online]. Available: https://packages.debian.org/sid/libssl-dev. [Accessed 31 July 2021].

[23] C. Hosmer, Python Forensics: A Workbench for Inventing and Sharing Digital Forensic Technology, Rockland Town, MA: Syngress Publishing, 2014.

[24] "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].

[25] A. Pradhan and R. Mathew, "Solutions to Vulnerabilities and Threats in Software Defined Networking (SDN)," *Procedia Computer Science,* vol. 171, p. 2585, 2020.

[26] 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].

[27] R. Chandel, "Wireless Penetration Testing Aircrack-ng," 08 July 2021. [Online]. Available: https://www.hackingarticles.in/wireless-penetration-testing-aircrack-ng. [Accessed 05 September 2021].

[28] T. d'Otreppe, "Aircrack-ng Repository," 22 November 2015. [Online]. Available: https://github.com/aircrack-ng/aircrack-ng. [Accessed 05 August 2021].

[29] "Kali Linux – Aircrack-ng," GeeksforGeeks, 08 July 2020. [Online]. Available: https://www.geeksforgeeks.org/kali-linux-aircrack-ng/. [Accessed 05 August 2021].

[30] L. Shinder and M. Cross, Scene of the Cybercrime, Rockland, MA: Syngress Publishing, 2008.

[31] J. Ludin, "EAP-TLS vs. PEAP-MSCHAPv2: Which Authentication Protocol is Superior?," SecureW2, 31 January 2020. [Online]. Available: https://www.securew2.com/blog/eap-tls-vs-peap-mschapv2-which-authentication-protocol-is-superior. [Accessed 12 August 2021].

[32] "NT LAN Manager Authentication Protocol," Microsoft, 07 April 2021. [Online]. Available: https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-nlmp/a4f28e01-3df1-4fd1-80b2-df1fbc183f21. [Accessed 13 August 2021].

[33] K. Sharkey, D. Coulter, D. Batchelor and M. Satran, "Microsoft NTLM," Microsoft, 31 May 2018. [Online]. Available: https://docs.microsoft.com/en-us/windows/win32/secauthn/microsoft-ntlm?redirectedfrom=MSDN. [Accessed 13 August 2021].

[34] J. Ludin, "WPA2-Enterprise Authentication Protocols Comparison," SecureW2, 03 October 2019. [Online]. Available: https://www.securew2.com/blog/wpa2-enterprise-authentication-protocols-comparison. [Accessed 13 August 2021].

[35] J. Wright, "asleap Repository," 10 May 2007. [Online]. Available: https://github.com/joswr1ght/asleap. [Accessed 13 August 2021].

[36] H. Singh, Kali Linux Wireless Pentesting and Security, New Delhi: rootsh3ll Labs, 2017.

[37] 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].

[38] Cisco Systems, Inc., "PMKID Vulnerability FAQ - WPA/WPA2-PSK and 802.11r," Cisco Meraki, 2020.

[39] P. Grubbs, "What is EAP-TLS?," SecureW2, 20 January 2021. [Online]. Available: https://securew2.com/blog/what-is-eap-tls. [Accessed 04 September 2021].

[40] J. Ludin, "Public Key Infrastructure: Explained," SecureW2, 30 September 2019. [Online]. Available: https://securew2.com/blog/public-key-infrastructure-explained. [Accessed 04 September 2021].