DAFTAR PUSTAKA

[1] BBC, "Facebook security app used to 'spy' on competitors," BBC, 18 Februari 2019. [Online]. Available: https://www.bbc.com/news/technology-47281906. [Accessed 11 Maret 2019].

[2] H. M. Rinanda, "Pelaku Skimming di Kediri Tertangkap," detik.com, 11 April 2018. [Online]. Available: https://news.detik.com/berita-jawa-timur/d-3966350/pelaku-skimming-atm-di-kediri-tertangkap. [Accessed 11 Maret 2019].

[3] B. M. M. Jai Narayan Goel, "Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology," in *3rd International Conference on Recent Trends in Computing 2015 (ICRTC-2015)*, Hyderabad, 2015.

[4] B. Dickson, "What is buffer overflow, an old vulnerability that's causing new problems?," The Daily Dot, 29 Mei 2019. [Online]. Available: https://www.dailydot.com/layer8/buffer-overflow-whatsapp/. [Accessed 22 November 2019].

[5] "CVE-2019-3568," MITRE Corporation, 13 Agustus 2019. [Online]. Available: https://www.cvedetails.com/cve/CVE-2019-3568/. [Accessed 22 November 2019].

[6] U. Saraf and S. K. Gupta, "Buffer Overflow Attacks & Countermeasures," 2007.

[7] T. Ahmed, "Study of Buffer Overflow on Dispersed Operating System Computing," 2005.

[8] D. Mbina, "Evaluation of Custom Tools for Pentest Automation," 2017.

[9] H. Azaim, "Mengenal Confidentiality, Integrity, dan Availability Pada Keamanan Informasi," NETSEC.ID, 5 Januari 2017. [Online]. Available: https://netsec.id/confidentiality-integrity-availability-keamanan-informasi/. [Accessed 2 September 2018].

[10] EC-Council, "Certified Ethical Hacking Workbook," *CEH v10:EC-Council Certified Ethical Hacker Complete Training Guide With Practice Labs,* p. 48, 14 Mai 2018.

[11] S. Watts, "IT Security Vulnerability vs Threat vs Risk: What are the Differences?," BMC Software, Inc., 21 Juni 2017. [Online]. Available: https://www.bmc.com/blogs/security-vulnerability-vs-threat-vs-risk-whats-difference/. [Accessed 24 November 2019].

[12] Cisco, "Finding Security Vulnerability," Cisco, [Online]. Available: https://static-course-assets.s3.amazonaws.com/CyberSec2.1/en/index.html#2.1.1.1. [Accessed 30 7 2019].

[13] Cisco, "Types of Attackers," Cisco, [Online]. Available: https://static-course-assets.s3.amazonaws.com/CyberSec2.1/en/index.html#1.3.1.1. [Accessed 30 07 2019].

[14] P. Bhunia, "NHS attack latest example of healthcare sector's vulnerability to Ransomware," OpenGov Asia, 27 Oktober 2017. [Online]. Available: https://www.opengovasia.com/nhs-attack-latest-example-of-healthcare-sectors-vulnerability-to-ransomware/. [Accessed 7 Desember 2019].

[15] D. Miessler, "The Difference Between Red, Blue, and Purple Teams," Daniel Miessler, 29 Agustus 2019. [Online]. Available: https://danielmiessler.com/study/red-blue-purple-teams/. [Accessed 25 November 2019].

[16] SecurityTrails Team, "Cybersecurity Red Team Versus Blue Team - Main Differences Explained," SecurityTrails, 7 Desember 2018. [Online]. Available: https://securitytrails.com/blog/cybersecurity-red-blue-team. [Accessed 25 11 2019].

[17] J. Fruhlinger, "Social engineering explained: How criminals exploit human behavior," CSO, IDG Communications, 25 September 2019. [Online]. Available: https://www.csoonline.com/article/2124681/what-is-social-engineering.html. [Accessed 25 November 2019].

[18] David Kennedy, Jim O'Gorman, Devon Kearns, Mati Aharoni, "Metasploit Basic," in *Metasploit, The Penetration Tester's Guide*, San Francisco, William Pollock, 2011, p. 8.

[19] David Kennedy, Jim O'Gorman, Devon Kearns, Mati Aharoni, "Introduction," in *Metasploit, The Penetration Tester's Guide*, San Francisco, William Pollock, 2011, p. xxii.

[20] TechTerms, "Digital Footprint," Sharpened Productions, 26 Mei 2014. [Online]. Available: https://techterms.com/definition/digital_footprint. [Accessed 26 November 2019].

[21] United States Nuclear Regulatory Commision, "www.nrc.gov - /docs/ML0502/," 11 November 2012. [Online]. Available: https://www.nrc.gov/docs/ML0502/. [Accessed 8 Desember 2019].

[22] R. Hertzog, J. O'Gorman and M. Aharoni, "Introduction," in *Kali Linux Revealed, Mastering the Penetration Testing Distribution*, Cornelius, Offsec Press, 2017, p. XIX.

[23] H. Dalziel, "Metasploit For Beginners," Concise AC, 13 Desember 2018. [Online]. Available: https://www.concise-courses.com/metasploit-for-beginners/. [Accessed 27 November 2019].

[24] D. Kennedy, J. O'Gorman, D. Kearns and M. Aharoni, "Building Your Own Module," in *Metasploit- The Penetration Tester's Guide*, San Francisco, No Starch Press, Inc., 2011, p. 185.

[25] Offensive Security, "Understanding Payloads in Metasploit," Offensive Security, [Online]. Available: https://www.offensive-security.com/metasploit-unleashed/payloads/. [Accessed 29 November 2019].

[26] Inference Security, "ICMP Reverse Shell," Infosec Resources, [Online]. Available: https://resources.infosecinstitute.com/icmp-reverse-shell/. [Accessed 29 November 2019].

[27] Offensive Security, "Payload Types in The Metasploit Framework," Offensive Security, [Online]. Available: https://www.offensive-security.com/metasploit-unleashed/payload-types/. [Accessed 29 November 2019].

[28] Belajarpython, "Pendahuluan Python," Belajarpython, [Online]. Available: https://belajarpython.com/tutorial/apa-itu-python. [Accessed 31 Desember 2019].

[29] GCSE Computer Science , "Von Neumann Architecture," GCSE Computer Science , [Online]. Available: https://www.computerscience.gcse.guru/theory/von-neumann-architecture. [Accessed 8 Desember 2019].

[30] T. Satti, "The Basic Organization of Computers," SlideShare, 18 Januari 2016. [Online]. Available: https://www.slideshare.net/TallatSatti/the-basic-organization-of-computers. [Accessed 8 Desember 2019].

[31] E. Corniel, "The CPU and The Memory," Medium, 29 Agustus 2016. [Online]. Available: https://medium.com/@esmerycornielle/the-cpu-and-the-memory-2eb300d6c72d. [Accessed 8 Desember 2019].

[32] J. W. Bacon, "Memory Segments," University of Wisconsin, 2011. [Online]. Available: http://www.cs.uwm.edu/classes/cs315/Bacon/Lecture/HTML/ch10s04.html. [Accessed 7 Oktober 2019].

[33] EC-Council, "Ethical Hacking and Countermeasures," *CEHv8,* p. 2707, 2013.

[34] J. C. Foster, V. Osipov, N. Bhalla and N. Heinen, "Expanding on Buffer Overflows," in *Buffer Overflow Attacks. Detect, Exploit, Prevent.*, Rockland, Syngress, 2005, p. 3.

[35] T. Suliman, "Understanding Buffer-overflow Exploit," Medium, 22 August 2018. [Online]. Available: https://medium.com/@tamirsuliman/understanding-buffer-overflow-exploit-6fdf495c7d8d. [Accessed 29 August 2019].

[36] EC-Council, "Ethical Hacking and Countermeasures," *CEHv8,* p. 2699, 2013.

[37] Common Weakness Enumeration (CWE), "CWE-121: Stack-based Buffer Overflow," MITRE, 19 September 2019. [Online]. Available: https://cwe.mitre.org/data/definitions/121.html. [Accessed 20 Januari 2020].

[38] OWASP, "Format String Attack," OWASP, 16 04 2015. [Online]. Available: https://www.owasp.org/index.php/Format_string_attack. [Accessed 07 November 2019].

[39] R. Auger, "Integer Overflows," Web Application Security Consortium, 30 12 2009. [Online]. Available: http://projects.webappsec.org/w/page-revisions/13246946/Integer%20Overflows. [Accessed 07 November 2019].

[40] Agile Insider Blog, "Understanding Date Execution Prevention (DEP) as a Security Mitigation Strategy," AgileIT, 14 Juni 2009. [Online]. Available: https://www.agileit.com/news/understanding-date-execution-prevention-dep-as-a-security-mitigation-strategy/. [Accessed 13 Januari 2020].

[41] D. Stewart, "What is ASLR, and How Does It Keep Your Computer Secure," How To Geek, 26 Oktober 2016. [Online]. Available: https://www.howtogeek.com/278056/what-is-aslr-and-how-does-it-keep-your-computer-secure/. [Accessed 13 Januari 2020].

[42] Red Hat, "Stack Guard Page Circumvention Affecting Multiple Packages," Red Hat, 19 Juni 2017. [Online]. Available: https://access.redhat.com/security/vulnerabilities/stackguard. [Accessed 13 Januari 2020].

[43] Andre, "Tutorial Belajar C Part 1: Pengertian Bahasa Pemrograman C," DuniaIlkom, 2 September 2018. [Online]. Available: https://www.duniailkom.com/tutorial-belajar-c-pengertian-bahasa-pemrograman-c/. [Accessed 2 Desember 2019].

[44] the GDB developers, "GDB: The GNU Project Debugger," Free Software Foundation, 20 September 2019. [Online]. Available: https://www.gnu.org/software/gdb/. [Accessed 30 November 2019].

[45] longld, "PEDA - Python Exploit Development Assistance for GDB," github, 3 Juni 2013. [Online]. Available: https://github.com/longld/peda. [Accessed 1 Desember 2019].

[46] Immunity Inc., "Debugger," Immunity Inc., [Online]. Available: https://www.immunityinc.com/products/debugger/. [Accessed 31 Desember 2019].

[47] J. Haddix, "New to reversing? The differences between IDA Pro, ImmDBG and OllyDBG," jassonhaddix.com, 13 April 2011. [Online]. Available: https://jasonhaddix.com/new-to-reversing-the-differences-between-ida-pro-immdbg-and-ollydbg/. [Accessed 13 Januari 2020].

[48] "Assembly - Introduction," tutorialspoint, 2019. [Online]. Available: https://www.tutorialspoint.com/assembly_programming/assembly_introduction.htm. [Accessed 21 October 2019].

[49] J. Foster, V. Osipov and N. Bhalla, Buffero Overflow Attacks: Detect, Exploit, Prevent., Rockland: Syngress Publishing, 2005.

[50] TutorialsPoint, "Assembly - Registers," tutorialspoint, 2019. [Online]. Available: https://www.tutorialspoint.com/assembly_programming/assembly_registers.htm. [Accessed 21 October 2019].

[51] Creative Commons BY-ND, "Code Table >> OpCode of Intel Assembly 80x86," Creative Commons BY-ND, [Online]. Available: http://www.jegerlehner.ch/intel/opcode.html. [Accessed 24 November 2019].

[52] J. C. Foster, V. Osipov, N. Bhalla and N. Heinen, "An Overview of Shellcode," in *Buffer Overflow Attacks*, United States of Amerika, Syngress Publishing, 2015, p. 26.

[53] R. Srinivasan, "PROTECTING ANTI-VIRUS SOFTWARE UNDER VIRAL ATTACKS," 2007.

[54] Chris Anley, John Heasman, Felix Linder, Gerardo Richarte, "Shellcode," in *The Shellcoder's Handbook*, Indianapolis, Wiley Publishing, 2007, p. 41.

[55] S. Levi, "Windows/x86 - Reverse (127.0.0.1:4444/TCP) Shell + Staged + Alphanumeric Shellcode (332 bytes)," Offensive Security, 1 Maret 2017. [Online]. Available: https://www.exploit-db.com/exploits/41481. [Accessed 9 Desember 2019].

[56] Cyber Edu, "What is Sandbox Security?," Force Point, [Online]. Available: https://www.forcepoint.com/cyber-edu/sandbox-security. [Accessed 1 Desember 2019].

[57] J. Winston, "What are the pros and cons of VirtualBox versus QEMU," Quora, 8 Mei 2016. [Online]. Available: https://www.quora.com/What-are-the-pros-and-cons-of-VirtualBox-versus-QEMU. [Accessed 13 Januari 2020].

[58] L. A. Notenboom, "What's the Difference Between a Sandbox and a Virtual Machine?," Ask Leo!, 18 Januari 2012. [Online]. Available: https://askleo.com/whats-the-difference-between-a-sandbox-and-a-virtual-machine/. [Accessed 2 Desember 2019].

[59] Ad4msan, "Windows XP Pro SP-3 Update Juni 2019!!," Ad4msan, 22 Juni 2019. [Online]. Available: https://ad4msan.com/windows-xp-pro-sp-3-update-juni-2019. [Accessed 1 Januari 2020].

[60] M. Gelbmann, "Ubuntu became the most popular Linux distribution for web servers," W3Techs, 2 Mei 2016. [Online]. Available: https://w3techs.com/blog/entry/ubuntu_became_the_most_popular_linux_distribution_for_web_servers. [Accessed 2 12 2019].

[61] wpadminsrt, "What is an FTP Server?," Titan, 11 September 2018. [Online]. Available: https://titanftp.com/2018/09/11/what-is-an-ftp-server/. [Accessed 2 Desember 2019].

[62] BeritaBebas, "Common Vulnerabilities and Exposures (CVE)," BeritaBebas, [Online]. Available: https://www.beritabebas.com/definisi/common-vulnerabilities-and-exposures-cve/. [Accessed 1 Januari 2020].

[63] Mitre Corporation, "CVE-2013-4730," Mitre Corporation, 30 Desember 2016. [Online]. Available: https://www.cvedetails.com/cve/CVE-2013-4730/. [Accessed 1 Januari 2020].

[64] Computer Security Student, "PCMan's FTP Server 2.0.7 Buffer Overflow Explained," Computer Security Student, [Online]. Available: https://www.computersecuritystudent.com/SECURITY_TOOLS/BUFFER_OVERFLOW/WINDOWS_APPS/lesson1/index.html. [Accessed 1 Januari 2020].

[65] R. Herzog, J. O'Gorman and M. Aharoni, Kali Linux Revealed, Cornelius: Offsec Press, 2017.

[66] D. Kennedy, J. O'Gorman, D. Kearns and M. Aharoni, Metasploit The Penetration Tester Guide, San Francisco: William Pollock, 2011.

[67] J. Foster, V. Osipov and N. Bhalla, Buffer Overflow Attacks: Detect, Exploit, Prevent, Rockland: Syngress Publishing, 2005.

[68] C. Anley, J. Heasman, F. Linder and G. Richarte, The Shellcoder's Handbook Second Edition, Indianapolis: Wiley Publishing, 2007.

[69] David Kennedy, Jim O'Gorman, Devon Kearns, Mati Aharoni, "The Phases of the PTES," in *Metasploit, The Penetration Tester's Guide*, San Fransisco, William Pollock, 2011, p. 2.

[70] interserver, "WHOIS Lookup Explained," InterServer Inc, [Online]. Available: https://www.interserver.net/tips/kb/whois-lookup-explained/. [Accessed 2018 September 19].

[71] T. Nojima, "Exploiting Simple Buffer Overflow (3) - Writing a simple Metasploit module," Github, 24 Juli 2016. [Online]. Available: http://taishi8117.github.io/2016/07/24/bof-metasploit/. [Accessed 9 Desember 2019].

[72] Offensive Security, "MSFVENOM," Offensive Security, [Online]. Available: https://www.offensive-security.com/metasploit-unleashed/Msfvenom/. [Accessed 31 Desember 2019].

[73] Offensive Security, "Meterpreter Basic Commands," Offensive Security, [Online]. Available: https://www.offensive-security.com/metasploit-unleashed/meterpreter-basics/. [Accessed 6 Desember 2019].