

DAFTAR PUSTAKA

- [1] D. K. Rahmatullah, S. M. Nasution, and F. Azmi, "Implementation of low interaction web server honeypot using cubieboard," *ICCEREC 2016 - Int. Conf. Control. Electron. Renew. Energy, Commun. 2016, Conf. Proc.*, pp. 127–131, 2017, doi: 10.1109/ICCEREC.2016.7814970.
- [2] M. Nawrocki, M. Wählisch, T. C. Schmidt, C. Keil, and J. Schönfelder, "A Survey on Honeypot Software and Data Analysis," 2016, [Online]. Available: <http://arxiv.org/abs/1608.06249>.
- [3] B. R. Prasad, A. Abraham, V. Suhas, and K. Kumar, "DOS attack pattern generator for training the neural network based classifier to dynamically blacklist IP in honeypot based NIDS/NIPS," *Thinkquest~2010*, pp. 224–226, 2011, doi: 10.1007/978-81-8489-989-4_41.
- [4] N. Arkaan and D. V. S. Y. Sakti, "Implementasi Low Interaction Honeypot Untuk Analisa Serangan Pada Protokol SSH," *J. Nas. Teknol. dan Sist. Inf.*, vol. 5, no. 2, pp. 112–120, 2019, doi: 10.25077/teknosi.v5i2.2019.112-120.
- [5] B. Mardiyanto, T. Indriyani, and I. M. Suartana, "Analisis dan Implementasi Honeypot dalam Mendeteksi Serangan Distributed Denial-Of-Services (DDOS) pada Jaringan Wireless," *Integer J.*, vol. 1, no. 2, pp. 32–42, 2016.
- [6] A. W. Muhammad and I. Riadi, "Analisis Statistik Log Jaringan Untuk Deteksi," *Ilk. J. Ilm.*, vol. 8, no. 3, pp. 220–225, 2016.
- [7] Hudzaifah, A. Sularsa, and D. R. Suchendra, "Membangun Sistem Monitoring Malicious Traffic Di Jaringan Dengan Maltrail," *e-Proceeding Appl. Sci.*, vol. 4, no. 3, pp. 2013–2018, 2018.
- [8] Z. Amin, "Analisis Vulnerabilitas Host Pada Keamanan Jaringan Komputer Di Pt . Sumeks Tivi Palembang (Paltv) Menggunakan Router Berbasis Unix," *Teknol. dan Inform.*, vol. 2, no. 3, pp. 189–199, 2012.
- [9] J. B. Bolanio, R. K. Paredes, A. L. Yoldan Jr., and R. E. Acapulco II, "Network

- Security Policy for Higher Education Institutions based on ISO Standards,” *Mediterr. J. Basic Appl. Sci.*, vol. 05, no. 01, pp. 01–17, 2021, doi: 10.46382/mjbas.2021.5101.
- [10] L. P. Aidin, S. M. Nasution, and F. Azmi, “Implementasi High Interaction Honeypot Pada Implementation of High Interaction Honeypot,” *e-Proceeding Eng.*, vol. 3, no. 2, pp. 2172–2178, 2016.
- [11] N. Naik, P. Jenkins, N. Savage, and L. Yang, “A computational intelligence enabled honeypot for chasing ghosts in the wires,” *Complex Intell. Syst.*, vol. 7, no. 1, pp. 477–494, 2021, doi: 10.1007/s40747-020-00209-5.
- [12] M. Mueter, F. Freiling, T. Holz, and J. Matthews, “A generic toolkit for converting web applications into high-interaction honeypots,” *Univ. Mannheim*, 2008, [Online]. Available: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.89.5000&rep=rep1&type=pdf%5Cnpapers2://publication/uuid/3F63605B-8FF8-4A51-97F6-AF46226DD97C>.
- [13] D. W. Johnson *et al.*, “Application of Medihoney Antibacterial Wound Gel for the Prevention,” *Society*, vol. 29, no. 2, pp. 303–309, 2009.
- [14] J. Mack, Y.-H. (Frank) Hu, and M. A. Hoppa, “A Study of Existing Cross-Site Scripting Detection and Prevention Techniques Using XAMPP and VirtualBox,” *Va. J. Sci.*, vol. 70, no. 3, p. 1, 2019, doi: 10.25778/bx6k-2285.
- [15] D. Legay, A. Decan, and T. Mens, “On Package Freshness in Linux Distributions,” *Proc. - 2020 IEEE Int. Conf. Softw. Maint. Evol. ICSME 2020*, pp. 682–686, 2020, doi: 10.1109/ICSME46990.2020.00072.
- [16] R. T. Gaddam and M. Nandhini, “An analysis of various snort based techniques to detect and prevent intrusions in networks: Proposal with code refactoring snort tool in Kali Linux environment,” *Proc. Int. Conf. Inven. Commun. Comput. Technol. ICICCT 2017*, no. Icicct, pp. 10–15, 2017, doi: 10.1109/ICICCT.2017.7975177.
- [17] B. Korniyenko and L. Galata, “Implementation of the information resources

- protection based on the CentOS operating system,” *2019 IEEE 2nd Ukr. Conf. Electr. Comput. Eng. UKRCON 2019 - Proc.*, pp. 1007–1011, 2019, doi: 10.1109/UKRCON.2019.8879981.
- [18] N. S. Sulaiman, A. Shafiq, and H. Ahmad, “Comparison of Operating System Performance Between Windows 10 and Linux Mint,” vol. 2, no. 1, pp. 92–102, 2021.
- [19] lms.onnocenter.or.id, "Maltrail", 4 November 2018. <https://lms.onnocenter.or.id/wiki/index.php/Maltrail>.
- [20] Cnbcindonesia.com, "Cerita Lengkap Bocornya 91 Juta Data Akun Tokopedia", 4 Mei 2020. <https://www.cnbcindonesia.com/tech/20200504063854-37-155936/cerita-lengkap-bocornya-91-juta-data-akun-tokopedia>.
- [21] Kompas.com, "Data 279 Juta Penduduk Indonesia Diduga Bocor, Ini Kata Kominfo", 21 Mei 2021. <https://www.kompas.com/tren/read/2021/05/21/113000365/data-279-juta-penduduk-indonesia-diduga-bocor-ini-kata-kominfo?page=all>.
- [22] Github (2021) Readme.md[stamparm/maltrail]. <https://github.com/stamparm/maltrail/Readme.md>
- [23] Github (2021) Readme.md[shipcod3/honey.py]. <https://github.com/shipcod3/honey.py/Readme.md>