DAFTAR PUSTAKA

[1] O. Suryana, “Server dan Web Server,” no. August, hal. 14–23, 2018.

[2] F. U. Com, “Ebook fui forum ubuntu-indonesia.com,” 2011.

[3] R. Mentang, A. A. E. Sinsuw, X. B. N. Najoan, dan J. T. Elektro-ft, “Perancangan Dan Analisis Keamanan Jaringan Nirkabel Menggunakan Wireless Intrusion Detection System,” *E-Journal Tek. Elektro Dan Komput.*, vol. 5, no. 7, hal. 35–44, 2015.

[4] M. S. Hasibuan, “Keylogger pada Aspek Keamanan Komputer,” *Teknovasi*, vol. 3, no. 1, hal. 8–15, 2016.

[5] R. Hermawan, “Analisis Konsep Dan Cara Kerja Serangan Komputer Distributed Denial of Service (Ddos),” *Anal. Konsep Dan Cara Kerja Serangan Komput. Distrib. Denial Serv.*, vol. 5, no. 1, hal. 1–14, 2013.

[6] I. Gunawan, “Penggunaan Brute Force Attack Dalam Penerapannya Pada Crypt8 Dan Csa-Rainbow Tool Untuk Mencari Biss,” *InfoTekJar (Jurnal Nas. Inform. dan Teknol. Jaringan)*, vol. 1, no. 1, hal. 52–55, 2016, doi: 10.30743/infotekjar.v1i1.48.

[7] I. dkk Sari, “Sistem MOnitoring Serangan Jaringan Komputer Berbasis Web Service meggunakan Honeypot Sebagai Intrusion Prevention System,” vol. 5, no. 1, hal. 35–44, 2019.

[8] A. dkk Prima Lukito, “Implementasi High Interaction Honeypot Pada Server,” *E-Proceding of Enginering*, vol. 3, no. 2, hal. 21–22, 2016.

[9] S. Dowling, M. Schukat, dan E. Barrett, “Improving adaptive honeypot functionality with efficient reinforcement learning parameters for automated malware,” *J. Cyber Secur. Technol.*, vol. 2, no. 2, hal. 75–91, 2018, doi: 10.1080/23742917.2018.1495375.

[10] T. Sochor dan M. Zuzcak, “Study of Internet Threats and Attack Methods Using Honeypots and Honeynets,” *Commun. Comput. Inf. Sci.*, vol. 431, hal. 118–127, 2014, doi: 10.1007/978-3-319-07941-7_12.

[11] P. Yoga, “Implementasi Intrusion Prevention System (IPS) Menggunakan Snort dan IPtables,” *J. Manaj. Inform.*, vol. 7, no. 1, hal. 21–28, 2017.

[12] E. K. Dewi, “Analisis Log Snort Menggunakan Network Forensic,” *JIPI (Jurnal Ilm. Penelit. dan Pembelajaran Inform.*, vol. 2, no. 2, hal. 72–79, 2017, doi: 10.29100/jipi.v2i2.370.

[13] A. P. Wicaksono, J. Raya, D. Po, dan B. Purwokerto, “Sistem Deteksi Intrusi dengan Snort (Intrusion Detection System with Snort),” *J. Inform.*, vol. III, hal. 31–34, 2014, doi: 10.30595/juita.v3i1.850.

[14] S. V. Doshi, S. B. Pawar, A. G. Shelar, dan S. S. Kulkarni, “Artificial Intelligence Chatbot in Android System using Open Source Program-O,” *Ijarcce*, vol. 6, no. 4, hal. 816–821, 2017, doi: 10.17148/ijarcce.2017.64151.

[15] G. M. D’Silva, S. Thakare, S. More, dan J. Kuriakose, “Real world smart chatbot for customer care using a software as a service (SaaS) architecture,” *Proc. Int. Conf. IoT Soc. Mobile, Anal. Cloud, I-SMAC 2017*, hal. 658–664, 2017, doi: 10.1109/I-SMAC.2017.8058261.

[16] onnocenter, “IPv6 Security: Audit Security,” 2019. http://onnocenter.or.id/wiki/index.php/IPv6_Security:_Audit_Security#Security_auditing_menggunakan_zenmap (diakses Jul 21, 2020).