

## DAFTAR PUSTAKA

- [1] R. Suwanto, I. Ruslianto dan M. Diponegoro, “Implementasi Intrusion Prevention System (IPS) Menggunakan Snort dan Iptable Pada Monitoring Jaringan Lokal Berbasis Website,” *Coding Jurnal Komputer dan Aplikasi*, vol. 07, no. 01, pp. 97-107, 2019.
- [2] R. Agustin, I. Fitri dan N. D. Nathasia, “Implementasi Metode Intrusion Detection Systems (IDS) dan Intrusion Prevention Systems (IPS) Berbasis Snort Server Untuk Keamanan Jaringan LAN,” *Jurnal Informatika*, vol. 18, no. 1, pp. 71-84, 2018.
- [3] S. Jose, D. Malathi, B. Reddy dan D. Jayaseeli, “A Survey on Anomaly Based Host Intrusion Detection System,” *Journal of Physics: Conference Series*, vol. 1000, no. 1, p. 012049, 2018.
- [4] A. S. Fadhlillah, N. B. A. Karna dan A. I. Irawan, “Analisis Performansi Ids Menggunakan Metode Deteksi Anomaly-based Terhadap Serangan Dos,” *e-Proceedings of Engineering*, vol. 06, no. 02, pp. 3398-3405, Agustus 2019.
- [5] H. Suhendi dan W. D. Cahyo, “PERANCANGAN DAN IMPLEMENTASI KEAMANAN JARINGAN MENGGUNAKAN SNORT SEBAGAI INTRUSION PREVENTION SYSTEM (IPS) PADA JARINGAN INTERNET STEI ITB,” *Naratif: Jurnal Nasional Riset, Aplikasi dan Teknik Informatika*, vol. 03, no. 02, pp. 60-68, Desember 2021.
- [6] N. Adhiatma, *Master CCNA : Belajar Network itu Mudah*, Jakarta: Nirifa publisher, 2020, pp. 372-377.
- [7] A. Ghosh, J. K. Mandal dan R. Chakraborty, *Machine Learning Techniques and Analytics for Cloud Security*, Hoboken: Wiley, 2021, pp. 111-112.
- [8] GURUBARAN, “Intrusion Prevention System (IPS) In-depth Analysis – A Detailed Guide,” GBHackers on Security, 14 November 2021. [Online]. Available:

<https://gbhackers.com/intrusion-prevention-systemips-and-its-detailed-funtion-socsiem/>. [Diakses 5 September 2022].

- [9] A. Aldallal dan F. Alisa, “Effective Intrusion Detection System to Secure Data in Cloud Using Machine Learning,” *Symmetry*, vol. 13, no. 12, p. 2306, 2021.
- [10] S. J. Nendissa, Rusdin, R. Y. Tyaningsih, D. Thalib, I. Hasbi, I. S. Setianingsih, Afkar, M. N. Ghiffari, W. A. A. Praditasari dan E. L. Gaol, *PENGAJARAN BERBASIS TEKNOLOGI DIGITAL*, Bandung: Widina Bhakti Persada Bandung, 2022, p. 34.
- [11] M. Napizahni, “DDoS Attack: Pengertian, Jenis, dan Cara Mencegahnya,” *dewaweb*, 25 Desember 2021. [Online]. Available: <https://www.dewaweb.com/blog/ddos-attack-pengertian-dan-solusinya/>. [Diakses 23 Januari 2022].
- [12] W. Komputer, *Tutorial 5 Hari Belajar Hacking dari Nol*, Yogyakarta: ANDI, 2021, pp. 66-67.
- [13] A. Ohri, “Ping Flood or ICMP Flood Attack – A Simple Guide In 3 Points,” *jigsaw*, 13 Februari 2021. [Online]. Available: <https://www.jigsawacademy.com/blogs/cyber-security/ping-flood/>. [Diakses 7 Februari 2022].
- [14] M. U. Batoebara, *Teknologi Informasi Dan Komunikasi*, M. F. Zaini, Penyunt., Medan: UNDHAR PRESS, 2020, pp. 127-128.
- [15] M. Roesch, “Snort,” *Snort.org*, 2022. [Online]. Available: <https://www.snort.org/>. [Diakses 23 Januari 2022].
- [16] G. Comb, “Wireshark,” *Wireshark.org*, 2020. [Online]. Available: <https://www.wireshark.org/>. [Diakses 20 Juli 2022].
- [17] S. Shovon, “ethtool Commands and Examples,” *linuxhint*, 2018. [Online]. Available: [https://linuxhint.com/ethtool\\_commands\\_examples/#:~:text=ethtool%20is%20a%](https://linuxhint.com/ethtool_commands_examples/#:~:text=ethtool%20is%20a%20)

20networking%20utility,devices%20on%20your%20Linux%20computer.

[Diakses 22 Juli 2022].

[18] S. Sanfilippo, "Hping," Hping, 1 Januari 2018. [Online]. Available: <http://www.hping.org/>. [Diakses 20 Juli 2022].

[19] kali, "Hydra," KALI, 4 Mei 2022. [Online]. Available: <https://www.kali.org/tools/hydra/>. [Diakses 23 Juni 2022].

[20] doctorX, "Using the CUPP Tool to Generate Powerful Password Lists," CYBRARY, 6 Agustus 2021. [Online]. Available: <https://www.cybrary.it/blog/0p3n/using-cupp-tool-generate-powerful-password-lists/>. [Diakses 22 Juli 2022].

[21] M. Riadi, "Pengertian, Layanan dan Parameter Quality of Service (QoS)," kajianpustaka.com, 26 Mei 2019. [Online]. Available: <https://www.kajianpustaka.com/2019/05/pengertian-layanan-dan-parameter-quality-of-service-qos.html>. [Diakses 20 Juli 2022].