DAFTAR PUSTAKA

[1] Simon Kemp, “Digital 2024 Indonesia,” Datareportal. Diakses: 7 Mei 2024. [Daring]. Tersedia pada: https://datareportal.com/reports/digital-2024-indonesia

[2] Atikah Dhani Ayuningtyas, “Deteksi Serangan Distributed Denial Of Service (DDoS),” UIN Syarif Hidayatullah, Jakarta, 2023.

[3] Badan Siber dan Sandi Negara, “Laporan Tahunan Layanan Honeynet BSSN 2024,” 2023. Diakses: 7 Mei 2024. [Daring]. Tersedia pada: https://www.bssn.go.id/wp-content/uploads/2024/04/LAPTAH_HONEYNET_2023.pdf

[4] T. Ariyadi, A. Restu Mukti, dan H. Saputra, “Mitigation of Distributed Denial of Service (DDoS) Attacks on Software Defined Network (SDN) Architecture,” vol. 21, no. 4, hlm. 878–886, 2022.

[5] CNN Indonesia, “KPU Ungkap Situs Resmi Alami Ratusan Juta Serangan pada Pemilu 2024,” *CNN Indonesia*, Jakarta, 15 Februari 2024. Diakses: 10 Maret 2024. [Daring]. Tersedia pada: https://www.cnnindonesia.com/nasional/20240215005235-617-1062767/kpu-ungkap-situs-resmi-alami-ratusan-juta-serangan-pada-pemilu-2024

[6] Alibaba Clouder, “CIA Triad and SSH Brute-Forcing,” Alibaba Cloud. Diakses: 9 Maret 2024. [Daring]. Tersedia pada: https://www.alibabacloud.com/blog/cia-triad-and-ssh-brute-forcing_594914

[7] S. Ariyaningsih, A. A. Andrianto, A. surya Kusuma, dan Rezi, “Korelasi Kejahatan Siber Dengan Percepatan Digitalisasi Di Indonesia,” *Jurnal Ilmu Hukum Universitas Pasundan*, vol. 1, hlm. 1–12, Mei 2023.

[8] M. Affandi *dkk.*, “Implementasi Snort Sebagai Alat Pendeteksi Intrusi Menggunakan Linux,” *Jurnal Teknologi Informasi*, vol. 4, no. 2, hlm. 1–15, 2019, [Daring]. Tersedia pada: www.linux.org

[9] R. Amalia, T. U. Kalsum, dan R. Riska, “Analisis dan Implementasi Software Defined Networking (SDN) untuk Automasi Perangkat Jaringan,” *Infotek : Jurnal Informatika dan Teknologi*, vol. 4, no. 2, hlm. 312–322, Jul 2021, doi: 10.29408/jit.v4i2.3734.

[10] R. Firdaus, “Analisis Dan Implementasi High Interaction Honeypot Pada Server Skripsi,” Universitas Islam Riau, Riau, 2020.

[11] W. A. Prabowo, K. Fauziah, A. S. Nahrowi, M. N. Faiz, dan A. W. Muhammad, “Strengthening Network Security: Evaluation of Intrusion Detection and Prevention Systems Tools in Networking Systems,” *IJACSA) International Journal of Advanced Computer Science and Applications*, vol. 14, no. 9, 2023, [Daring]. Tersedia pada: www.ijacsa.thesai.org

[12] H. Wang dan B. Wu, “SDN-based hybrid honeypot for attack capture,” *IEEE 3rd Information Technology,Networking,Electronic and Automation Control Conference*, hlm. 1602–1606, 2019.

[13] U. Ubaidillah, T. Taryo, dan A. Hindasyah, “Analisis dan Implementasi Honeypot Honeyd Sebagai Low Interaction Terhadap Serangan Distributed Denial Of Service (DDOS) dan Malware,” *JTIM : Jurnal Teknologi Informasi dan Multimedia*, vol. 5, no. 3, hlm. 208–217, Okt 2023, doi: 10.35746/jtim.v5i3.405.

[14] H. Melhem dan Y. Dayoub, “A Hybrid Honeypot Framework for DDOS Attacks Detection and Mitigation,” *International Journal of Engineering Research & Technology (IJERT)*, Nov 2022, [Daring]. Tersedia pada: www.ijert.org

[15] J. Tamalaki Ohyver dan D. W. Chandra, “Simulasi Keamanan Jaringan pada DPDK OpenvSwitch Berbasis Network-Based Intrusion Detection System (NIDS),” *Universitas Kristen Satya Wacana*, vol. 7, no. 3, Feb 2023, doi: 10.35870/jti.

[16] Tati Ernawati dan Fikri Faiz Fadhlur Rachmat, “Keamanan Jaringan dengan Cowrie Honeypot dan Snort Inline-Mode sebagai Intrusion Prevention System,” *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, vol. 5, no. 1, hlm. 180–186, Feb 2021, doi: 10.29207/resti.v5i1.2825.

[17] M. Mispriatin, J. Gusti, A. Ginting, B. Arifwidodo, dan K. Kunci, “Analisis Kinerja Honeypot Dionaea Dan Cowrie Dalam Mendeteksi Serangan,” *Seminar Nasional TEKNOKA ke - 6 Vol. 6, 2021*, vol. 6, hlm. 2021, Nov 2021.

[18] et al I Gede Suputra Widharma, “Pengamanan Sistem Jaringan Komputer Dengan Teknologi Firewall,” Des 2020. [Daring]. Tersedia pada: https://www.researchgate.net/publication/346965331

[19] M. B. Firmansyah, R. M. Negara, dan D. D. Sanjoyo, "Mengimplementasikan Sistem Keamanan Jaringan Intrusion Prevention System Berbasis Snort Pada Arsitektur Software Defined Network," *Core Academy United Kingdom*, 2019.

[20] M. Iqbal dan M. Arif Ramadhan, "Analisa Quality of Service pada Jaringan Wireless Berbasis Software-Defined Network dengan Protokol Openflow Menggunakan Floodlight Controller," 2020.

[21] S. Yoga, "Analisis Performansi Software Defined Network (SDN)," Universitas Islam Riau, Riau, 2021.

[22] F. Yasin, Abdul Fadlil, dan Rusydi Umar, "Identifikasi Bukti Forensik Jaringan Virtual Router Menggunakan Metode NIST," *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, vol. 5, no. 1, hlm. 91–98, Feb 2021, doi: 10.29207/resti.v5i1.2784.

[23] B. Dodiya dan U. K. Singh, "Malicious Traffic analysis using Wireshark by collection of Indicators of Compromise," *Int J Comput Appl*, vol. 183, no. 53, hlm. 1–6, Feb 2022, doi: 10.5120/ijca2022921876.

[24] M. H. Asadullah, "Sistem Keamanan Server Dengan Honeypot Dan Intrusion Detection System (IDS) (Studi Kasus Perusahaan Printing Somatex)," Universitas Sebelas Maret, Surakarta, 2019. Diakses: 22 Maret 2024. [Daring]. Tersedia pada: https://core.ac.uk/download/pdf/211786224.pdf

[25] A. A. A. Suliman, "Implementasi Honeypot Dan Port Knocking Dalam Mendeteksi Serangan DDoS Attack Pada Sserver Jaringan," *SemanTIK : Teknik Informasi*, vol. 7, no. 1, hlm. 1–5, Jan 2021, doi: 10.5281/zenodo.5034918.

[26] Ilham Fitra Pradana, "Deteksi Keamanan Server Menggunakan Cowrie Dan Fortigate Pada Web Server Skripsi," Universitas Islam Negeri Syarif Hidayatullah, 2023.

[27] E. Chovancová dan N. Ádám, "A Clustered Hybrid Honeypot Architecture," Kosice, Jan 2019. doi: 10.12700/APH.16.10.2019.10.11.

[28] Meilinaeka, "VM (Virtual Machine), Wujud Kecangghian Dunia Digital," Website Telkom University. Diakses: 3 Maret 2024. [Daring]. Tersedia pada: https://it.telkomuniversity.ac.id/vm-virtual-machine-wujud-kecanggihan-dunia-digital/

[29] L. R. Kalluru, “Implementing Programmable Data Plane in Open vSwitch using P4 language,” Iowa State University, Iowa, 2023. Diakses: 12 Maret 2024. [Daring]. Tersedia pada: https://dr.lib.iastate.edu/server/api/core/bitstreams/82f3d70e-e27d-4a5b-a081-e9e8d8e62dd1/content

[30] M. Alsaeedi, M. M. Mohamad, dan A. A. Al-Roubaiey, “Toward Adaptive and Scalable OpenFlow-SDN Flow Control: A Survey,” *IEEE Access*, vol. 7, hlm. 107346–107379, 2019, doi: 10.1109/ACCESS.2019.2932422.

[31] A. Vishnu Priya dan N. Radhika, “Performance comparison of SDN OpenFlow controllers,” 2019. [Daring]. Tersedia pada: http://www.traffic.comics.unina.it/software/ITG/

[32] Network Data Sistem, “Apa Itu Open Network? Solusi Atasi Budget,” Network Data Sistem. Diakses: 2 Juli 2024. [Daring]. Tersedia pada: https://nds.id/apa-itu-open-network/

[33] M. Stubbig, *Practical OPNsense*, 4 ed. BookRix GmbH & Co. KG, 2019. Diakses: 29 Oktober 2024. [Daring]. Tersedia pada: https://github.com/practical-opnsense/practical-opnsense.github.io

[34] Adam Fahsyah Nurzaman, “Sistem Deteksi dan Pencegahan Intrusi,” School Of Information System. Diakses: 12 Maret 2024. [Daring]. Tersedia pada: https://sis.binus.ac.id/2020/12/09/sistem-deteksi-dan-pencegahan-intrusi/

[35] A. R. Gunawan, N. P. Sastra, dan D. M. Wiharta, “Penerapan Keamanan Jaringan Menggunakan Sistem Snort dan Honeypot Sebagai Pendeteksi dan Pencegah Malware,” *Majalah Ilmiah Teknologi Elektro*, vol. 20, no. 1, hlm. 81, Mar 2021, doi: 10.24843/mite.2021.v20i01.p09.

[36] T. Ariyadi, A. Restu Mukti, dan H. Saputra, “Mitigation of Distributed Denial of Service (DDoS) Attacks on Software Defined Network (SDN) Architecture,” vol. 21, no. 4, hlm. 878–886, 2022.

[37] L. Feronika Nainggolan, N. F. Saragih, F. G. N. Larosa, dan H. Artikel, “Monitoring Keamanan Jaringan Pada Server Ubuntu Dari Serangan DDoS Menggunakan Snort IDS,” vol. 2, no. 2, hlm. 1–10, 2022, [Daring]. Tersedia pada: http://ojs.fikom-methodist.net/index.php/METHOTIKA

[38] D. Miessler, “Password Lists,” Github. [Daring]. Tersedia pada: https://github.com/danielmiessler/SecLists/blob/master/Passwords/Common-Credentials/10-million-password-list-top-1000.txt

[39] Hardian Alkori, “GitHub - iyxn_honeypot,” Github. Diakses: 8 September 2024. [Daring]. Tersedia pada: https://github.com/iyxn/honeypot