

## DAFTAR PUSTAKA

- [1] S. Boddy, "Spaceballs Security: The Top Attacked Usernames and Passwords," F5, 20 12 2018. [Online]. Available: <https://www.f5.com/labs/articles/threat-intelligence/spaceballs-security--the-top-attacked-usernames-and-passwords>. [Accessed 24 12 2020].
- [2] Devi Afriyantari Puspa Putri, Aulia Rachmawati, "Honeypot Cowrie Implementation to Protect SSH Protocol in Ubuntu Server with Visualisation Using Kippo-Graph," *International Journal of Advanced Trends in Computer Science and Engineering*, Vols. Volume 8, No.6, pp. 3200-3207, 2019.
- [3] Jodi Chris Jordan Sihombing, Dany Primanita Kartikasari, Adhitya Bhawiyuga , "Implementasi Sistem Deteksi dan Mitigasi Serangan Distributed Denial of Service (DDoS) menggunakan SVM Classifier pada Arsitektur SoftwareDefined Network (SDN)," *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer* , 2019.
- [4] Pratita, Hanif Sidiq, "Analisa Brute Force Attack menggunakan Scanning Aplikasi pada HTTP Attack," Repository UKSW, Salatiga, 2016.
- [5] Sulaksono, Wahyu Adi, "Implementasi Honeypot Sebagai Sistem Keamanan Jaringan Pada Virtual Private Server," *Jurnal Nasional Informatika dan Teknologi Jaringan*, 2020.
- [6] Elang Dwi Saputro, Yudha Purwanto, Muhammad Faris Ruriawan, "PERANCANGAN DAN IMPLEMENTASI HONEYPOT PADA PERANGKAT INTERNET OF THINGS (IOT)," 2020.
- [7] Rizal Cerdas Kurniawan, Rohmat Tulloh, S.T., M.T., Dr. Indrarini Dyah Irawai S.T., M.T., "IMPLEMENTASI VPLS PADA JARINGAN SOFTWARE DEFINED NETWORK (SDN) DENGAN MENGGUNAKAN ONOS CONTROLLER BERBASIS RASPBERRY-PI 3," vol. 06, pp. 3796-3805, 2020.
- [8] Xupeng Luo, Qiao Yan , Mingde Wang , Wenyao Huang, "Using MTD and SDN-based Honeypots to Defend DDoS Attacks in IoT," *IEEE*, pp. 392-395, 2019.
- [9] Bagus Mardiyanto, Tutuk Indriyani, I Made Suartana, "Analisis Dan Implementasi Honeypot Dalam Mendeteksi Serangan Distributed Denial-Of-Services (DDOS) Pada Jaringan Wireless," *Integer Journal*, Vols. Vol 1, No 2, pp. 32-42, 2016.
- [10] Oosterhof, Michel, "Cowrie," 2014. [Online]. Available: <https://github.com/cowrie/cowrie>. [Accessed 5 2 2021].
- [11] Tati Ernawati, Fikri Faiz Fadhlur Rachmat, "Keamanan Jaringan dengan Cowrie Honeypot dan Snort Inline-Mode sebagai Intrusion Prevention System," *RESTI*, vol. Vol. 5, 2021.
- [12] Phuong M. Cao, Yuming Wu, Subho S. Banerjee, Justin Azoff,, Alexander Withers, Zbigniew T. Kalbarczyk, Ravishankar K. Iyer, "CAUDIT: Continuous Auditing of SSH Servers To Mitigate

Brute-Force Attacks," *Proceedings of the 16th USENIX Symposium on Networked Systems Design and Implementation*, pp. 1-25, 2019.

- [13] Seema Rani, Ritu Nagpal, "Penetration Testing Using Metasploit Framework : An Ethical Approach," *IRJET*, vol. 06, no. 08, pp. 538-542, 2019.
- [14] Community, Ryu SDN Framework, "COMPONENT-BASED SOFTWARE DEFINED NETWORKING FRAMEWORK," Ryu SDN Framework Community, 2014. [Online]. Available: <https://ryu-sdn.org/>. [Accessed 16 3 2021].
- [15] Novandha Yudyanto, Syaifuddin, Yufis Azhar, "Integrasi Modern Honey Network Dengan Grafana Untuk Visualisasi," *Vols. Vol. 2, No. 10*, no. 2714-7975, pp. 1380-1389, 2020.
- [16] Fahmi, Hasanul, "ANALISIS QOS (QUALITY OF SERVICE) PENGUKURAN DELAY, JITTER, PACKET LOST DAN THROUGHPUT UNTUK MENDAPATKAN KUALITAS KERJA RADIO STREAMING YANG BAIK," *TEKNOLOGI INFORMASI DAN KOMUNIKASI*, vol. Vol.7 No. 2, pp. 98 - 105, 2018.
- [17] Teguh Indra Bayu, Etwan Ewaldo Tahan, "Simulasi Konsep Software Defined Network (SDN) Menggunakan Raspberry Pi," *JUTEI*, vol. Volume.2 No.2, 2018.
- [18] Rahalkar, Sagar, *Quick Start Guide to Penetration Testing\_ With NMAP, OpenVAS and Metasploit*, Pune, Maharashtra, India: Apress, 2018.
- [19] Roby Rupiat, Sutan Faisal, Tohirin Al Mudzakir, Santi Arum Puspita Lestari1, "DETEKSI SERANGAN PERETAS MENGGUNAKAN HONEYPOT COWRIE DAN INTRUSION DETECTION SYSTEM SNORT," *CIASTECH 2020*, 2020.
- [20] Karolus Thias Widagdo, Teguh Indra Bayu, Yeremia Alfa Susetyo, "Pemodelan Sistem Monitoring Sensor Curah Hujan Menggunakan Grafana," *Indonesian Journal of Computing and Modelling*, vol. Volume 2 Nomor 2, pp. 1-8, 2018.