

DAFTAR PUSTAKA

- Almaleki, M. A. (United A. E. U. (2016). *Enhancing snort IDS performance using data mining. Digital Communications and Networking Commons.*
- Ananta, A. Y. P. N. M. (2017). Seleksi Notifikasi Serangan Berbasis IDS Snort. *SMARTICS Journal*, 3(2), 31–38.
- Christine, E. J., Hadi, M. Z. S., & Kusumaningtyas, E. M. (Teknologi S. N. (ITS) S. (2011). Aplikasi hierarchical clustering pada intrusion detection system berbasis snort, 6.
- Cvitić, I., Peraković, D., Periša, M., & Musa, M. (2017). Network Parameters Applicable in Detection of Infrastructure Level DDoS Attacks. *25th Telecommunications Forum TELFOR 2017*, (November). <https://doi.org/10.1109/TELFOR.2017.8249347>
- Di, P., Dari, I., & Hakim, P. (2015). Eksistensi alat bukti elektronik dalam sistem hukum pembuktian di indonesia dari perspektif hakim, 8(1), 1–29.
- Devisi Penelitian dan Pengembangan MADCOMS, Dasar Teknis Instalasi Jaringan Komputer, Penerbit ANDI, Yogyakarta, 2003.
- Diansyah, T. M. (Sekolah T. T. H. (2015). Analisa pencegahan aktivitas ilegal didalam jaringan menggunakan wireshark, *IV*(2), 20–23.
- Fadlil, A., Riadi, I., Aji, S., & Dahlan, U. A. (2017). Pengembangan sistem pengaman jaringan komputer berdasarkan analisis forensik jaringan, 3(1).
- Gondohanindijo, J. (2011). Sistem Untuk Mendeteksi Adanya Penyusup (IDS : Intrusion Detection System). *Semarang*, 2, 46–54.
- Handayana, W.B.T., Renaldy, B., Ashari, A., 2009. *Linux Sistem Administrator. Informatika, Bandung.*
- Hendra, U. P. N. “Veteran” Y. (2017). Pengembangan Teknologi Single Account Menggunakan Web Service Dan Lightweight Directory Access Protocol (Ldap) (Studi Kasus : Moodle Dan Wordpress), 128.
- Heryanto, A., Stiawan, D., & Napsiah. (2016). Visualisasi Serangan Denial Of Service Dengan Clustering Menggunakan K-Means Algorithm. *ANNUAL RESEARCH SEMINAR 2016*, 2(1), 348–354.
- Israelsson, P. (2005). A quick overview of Snort, 1–5.
- Koswara, E., 2012. *Jurus Kilat Mahir Ubuntu. Dunia Komputer, Bekasi.*
- Kristanto, Andri, *Jaringan Komputer, Penerbit Graha Ilmu, Yogyakarta, 2003.*

- Naik, N. (2015). Fuzzy Inference Based Intrusion Detection System : *IEEE International Conference on Computer and Information Technology*.
<https://doi.org/10.1109/CIT/IUCC/DASC/PICOM.2015.306>
- Nugroho, I. W. (2014). RANCANG BANGUN APLIKASI INTRUSSION DETECTION SYSTEM DENGAN MENGGUNAKAN METODE FUZZY, *1*, 103.
- Pradipta, Y. W. (U. N. S. (2017). IMPLEMENTASI INTRUSION PREVENTION SYSTEM (IPS) MENGGUNAKAN SNORT DAN IP TABLES BERBASIS LINUX, *7*(1), 21–28.
- Prasad, K. M., Mohan, A. R., & Jyothsna, R. V. (2012). IP Traceback for Flooding attacks on Internet Threat Monitors (ITM) Using Honeypots, *4*(1), 13–27.
- Pressman, R. S. (2010). *Software Engineering* (7th ed.). New York: McGraw-Hill.
- Riadi, I. (2014). *FRAMEWORK UNTUK FORENSIK INTERNET MENGGUNAKAN K-MEANS CLUSTERING DAN HORIZONTAL PARTITIONING*. Universitas Gadjah Mada Yogyakarta.
- Riadi, I., Istiyanto, J. E., Ashari, A., & Subanar. (2013). Internet Forensics Framework Based-on Clustering. *International Journal of Advanced Computer Science and Applications*, *4*, 115–123. <https://doi.org/10.14569/IJACSA.2013.041217>
- Sauter, M. (2013). “LOIC Will Tear Us Apart”: The Impact of Tool Design and Media Portrayals in the Success of Activist DDOS Attacks. *American Behavioral Scientist*, *57*(7), 983–1007. <https://doi.org/10.1177/0002764213479370>
- Singh, A., Rana, A., & Pradesh, U. (2013). K-means with Three different Distance Metrics, *67*(10), 13–17.
- Sofana, I. (2014). Cisco CNNA & Jaringan Komputer (Edisi revisi), Informatika Bandung, Bandung.
- Sommerville, I. (2011). *Software Engineering*. (Michael Hirsch, Ed.) (9th ed). United States of America: Addison Wesley.
- Subbulakshmi, T., Shalinie, S. M., Reddy, C. S., & Ramamoorthi, A. (n.d.). Detection and Classification of DDoS Attacks Using, 242–252.
- Suyanto, A. H. (2004). PENGENALAN JARINGAN KOMPUTER.
- Waskita, M. A., & Hiswendari, L. (2004). Local Area Network, 55.
- _____, Document snort <https://www.snort.org/documents> (Diakses pada 25 September 2019).