

DAFTAR PUSTAKA

- [1] Cimpanu, Catalin (Aug 30, 2016). "There's a 120,000-Strong IoT DDoS Botnet Lurking Around". Softpedia. Retrieved 19 October 2016.
- [2] "Attack of Things!". Level 3 Threat Research Labs. 25 August 2016. Retrieved 6 November 2016.
- [3] M. Zelkowitz, "New programming paradigms," vol. 64, Academic Press, 2005.
- [4] Teerawat Issariyakul, Ekram Hossain, Introduction to Network Simulator NS2, New York: Springer, 2012.
- [5] M. Aldo Shauma, Yudha Purwanto, Astri Novianty, "Deteksi Anomali Trafik Menggunakan Algoritma BIRCH dan DBSCAN pada STREAMING TRAFFIC", *Telkom University Final Project*, 2016.
- [6] Esraa Alomari, B. B. Gupta, Shankar Karuppayah, dkk. "Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art", *International Journal of Computer Applications*, 7 Juli 2012.
- [7] TEAM CYMRU. "DDoS Basics". Amerika Serikat. 22 Maret 2010
- [8] Jose Nazario. "BlackEnergy DDoS Bot Analysis". Oktober 2007
- [9] Lenny Hansson, Bjarne bachmann, dkk. "The BlackNurse Attacks". Denmark. 8 Nopember 2016.
- [10] HUAWEI TECHNOLOGIES CO., LTD. "2013 Botnets and DDoS Attacks Report". Shenzhen, China. 2013
- [11] Sobh, T. S. (2006). *Wired and wireless intrusion detection system: Classifications, good characteristics and state-of-the-art*. science@direct (pp. 1-25). Computer Standards & Interfaces.
- [12] Feily, M., Shahrestani, A., & Ramadass, S. (2009). *A Survey of Botnet and Botnet Detection*. Third International Conference on Emerging Security Information, Systems and Technologies (pp. 268-273). IEEE.
- [13] E. Council, "Denial of Service," in *Ethical Hacking and Countermeasures v7.1*, 2011, pp. 433-440.

- [14] Bächer, P., Holz, T., Kötter, M., & Wicherski, G. (2005). *Know your enemy: Tracking Botnets*. The HoneyNet Project. 1-21.
- [15] J. Matthew. (2002). "A Method For Mitigating Denial of Service Attacks on Differentiated Service Network". California, Amerika Serikat. September 2002