

## DAFTAR RUJUKAN

- Amor, N. Ben, Benferhat, S., & Elouedi, Z. (2004). Naive Bayes vs decision trees in intrusion detection systems. *Proceedings of the ACM Symposium on Applied Computing, 1*, 420–424.
- Atamli, A. W., & Martin, A. (2014). Threat-based security analysis for the internet of things. *Proceedings - 2014 International Workshop on Secure Internet of Things, SIoT 2014*. <https://doi.org/10.1109/SIoT.2014.10>
- Atmojo, Y. P. (2018). Analisa Performa Raspberry Pi sebagai Intrusion Detection System: Studi Kasus IDS Pada Server Web. *Eksplora Informatika*, 8(1), 24. <https://doi.org/10.30864/eksplora.v8i1.143>
- Bharathi, E. (2019). Intrusion Detection Using Raspberry Pi Honeypot ( Snort ) for Network Security. *International Research Journal of Engineering and Technology (IRJET)*, 479–481.
- Dewi, E. K., Harini, D., & Miftachurohmah, N. (2017). *Snort Ids Sebagai Tools Forensik Jaringan Universitas Nusantara PGRI Kediri*. January, 411–418.
- Hossain, M. M., Fotouhi, M., & Hasan, R. (2015). Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things. *Proceedings - 2015 IEEE World Congress on Services, SERVICES 2015, July*, 21–28. <https://doi.org/10.1109/SERVICES.2015.12>
- Kanagalakshmi, R., & Raj, V. N. (2014). *Network Intrusion Detection Using Hidden Naive Bayes Multiclass Classifier Model*. 03, 76–84.
- Manshour, N., Masoud Maleki, & Temel Kayıkçıoğlu. (2017). Network Forensics For Detecting Flooding Attack on Web Server. *International Journal of Computer Science and Information Security*, 15(2), 326–331. [https://www.researchgate.net/publication/315665126\\_Network\\_Forensics\\_For\\_Detecting\\_Flooding\\_Attack\\_On\\_Web\\_Server](https://www.researchgate.net/publication/315665126_Network_Forensics_For_Detecting_Flooding_Attack_On_Web_Server)
- Mukherjee, S., & Sharma, N. (2012). Intrusion Detection using Naive Bayes Classifier with Feature Reduction. *Procedia Technology*, 4, 119–128. <https://doi.org/10.1016/j.protcy.2012.05.017>
- Panda, M., & Patra, M. R. (2007). Network Intrusion Detection Using Naïve Bayes. *IJCSNS International Journal of Computer Science and Network Security*, 7(12), 258–263.
- Prasetyo, A., Affandi, L., & Arpandi, D. (2018). Implementasi metode naive bayes untuk intrusion detection system (ids). *Jurnal Informatika Polinema*, 4, 280–

284. <https://media.neliti.com/media/publications/266753-implementasi-metode-naive-bayes-untuk-in-803a0158.pdf>
- Ridho, F., Yudhana, A., & Riadi, I. (2016). *Analisis Forensik Router Untuk Mendeteksi Serangan Distributed Denial of Service (DDoS) Secara Real Time*. 2(1), 111–116. <http://ars.ilkom.unsri.ac.id>
- Rohokale, V. M., Prasad, N. R., & Prasad, R. (2011). A cooperative Internet of Things (IoT) for rural healthcare monitoring and control. *2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace and Electronic Systems Technology, Wireless VITAE 2011, May 2014*. <https://doi.org/10.1109/WIRELESSVITAE.2011.5940920>
- Sobari, I. A. (2015). Rancangan Wireless Intrusion Detection System Menggunakan Snort. *None*, 12(1), 1–9.
- Ulfa, M., Jenderal, J., Yani, A., & Palembang, N. (2013). *Implementasi Intrusion Detection System (IDS) Di Jaringan Internet Universitas Bina Darma*. 12, 105–118.
- Wahba, Y., ElSalamouny, E., & ElTaweel, G. (2015). *Improving the Performance of Multi-class Intrusion Detection Systems using Feature Reduction*. JUNE. <http://arxiv.org/abs/1507.06692>
- Wijatsongko, E. N., Putra, A. E., & Prastowo, B. N. (2015). Sistem Pemantauan Ruang dengan Server Raspberry Pi. *IJEIS (Indonesian Journal of Electronics and Instrumentation Systems)*, 5(1), 65. <https://doi.org/10.22146/ijeis.7154>
- Witten, I. H., Frank, E., & Hall, M. a. (2011). Data Mining: Practical Machine Learning Tools and Techniques (Google eBook). In *Complementary literature None*. <http://books.google.com/books?id=bDtLM8CODsQC&pgis=1>
- Zawoad, S., & Hasan, R. (2013). *Cloud Forensics: A Meta-Study of Challenges, Approaches, and Open Problems*. February 2013. <http://arxiv.org/abs/1302.6312>