DAFTAR PUSTAKA

[1] S. Hawkins, D. C. Yen, and D. C. Chou, "Awareness and challenges of Internet security," *Inf. Manag. Comput. Secur.*, vol. 8, no. 3, pp. 131–143, 2000.
[2] "Microsoft Security Intelligence Report Volume 21," Microsoft, Jun. 2016.
[3] S. Sharma and R. Gupta, "Intrusion Detection System: A Review," *Int. J. Secur. Its Appl.*, vol. 9, no. 5, pp. 69–76, 2015.
[4] A. Chandrasekhar and K. Raghuveer, "Intrusion detection technique by using k-means, fuzzy neural network and SVM classifiers," presented at the Computer Communication and Informatics (ICCCI), 2013 International Conference on, 2013, pp. 1–7.
[5] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, "Network anomaly detection: methods, systems and tools," *IEEE Commun. Surv. Tutor.*, vol. 16, no. 1, pp. 303–336, 2014.
[6] P. Mehra, "A brief study and comparison of snort and bro open source network intrusion detection systems," *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 1, no. 6, pp. 383–386, 2012.
[7] L. Dali *et al.*, "A survey of intrusion detection system," in *Web Applications and Networking (WSWAN), 2015 2nd World Symposium on*, 2015, pp. 1–6.
[8] P. Aggarwal and S. K. Sharma, "A Metric for Ranking the Classifiers for Evaluation of Intrusion Detection System," presented at the Proceedings of the Second International Conference on Computer and Communication Technologies, 2016, pp. 459–467.
[9] R. Mishra and A. Choubey, "Discovery of frequent patterns from web log data by using FP-growth algorithm for web usage mining," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 2, no. 9, 2012.
[10] A. N. Singh, S. Kumar, and R. C. Joshi, "Intrusion Detection System Based on Real Time Rule Accession and Honeypot," in *Advances in Network Security and Applications: 4th International Conference, CNSA 2011, Chennai, India, July 15-17, 2011*, D. C. Wyld, M. Wozniak, N. Chaki, N. Meghanathan, and D. Nagamalai, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 292–301.
[11] A. Sagala, "Automatic SNORT IDS rule generation based on honeypot log," in *2015 7th International Conference on Information Technology and Electrical Engineering (ICITEE)*, 2015, pp. 576–580.
[12] N. Fallahi, A. Sami, and M. Tajbakhsh, "Automated flow-based rule generation for network intrusion detection systems," in *2016 24th Iranian Conference on Electrical Engineering (ICEE)*, 2016, pp. 1948–1953.
[13] S. Lee *et al.*, "LARGen: Automatic Signature Generation for Malwares Using Latent Dirichlet Allocation," *IEEE Trans. Dependable Secure Comput.*, vol. PP, no. 99, pp. 1–1, 2016.
[14] C.-B. Jiang, I.-H. Liu, Y.-N. Chung, and J.-S. Li, "Novel intrusion prediction mechanism based on honeypot log similarity," *Int. J. Netw. Manag.*, vol. 26, no. 3, pp. 156–175, 2016.
[15] C. N. Kao *et al.*, "Automatic NIDS Rule Generating System for Detecting HTTP-like Malware Communication," in *2015 International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP)*, 2015, pp. 199–202.
[16] R. Koch and M. Golling, "Architecture for evaluating and correlating NIDS in real-

World networks," presented at the Cyber Conflict (CyCon), 2013 5th International Conference on, 2013, pp. 1–20.

[17] C. Musca, E. Mirica, and R. Deaconescu, "Detecting and Analyzing Zero-Day Attacks Using Honeypots," presented at the 2013 19th International Conference on Control Systems and Computer Science, 2013, pp. 543–548.

[18] T. Xing, D. Huang, L. Xu, C.-J. Chung, and P. Khatkar, "Snortflow: A openflow-based intrusion prevention system in cloud environment," presented at the Research and Educational Experiment Workshop (GREE), 2013 Second GENI, 2013, pp. 89–92.

[19] U. Oktay and O. K. Sahingoz, "Proxy network intrusion detection system for cloud computing," presented at the Technological Advances in Electrical, Electronics and Computer Engineering (TAEECE), 2013 International Conference on, 2013, pp. 98–104.

[20] F. L. Catherine, R. Pathak, and V. Vaidehi, "Efficient host based intrusion detection system using Partial Decision Tree and Correlation feature selection algorithm," presented at the Recent Trends in Information Technology (ICRTIT), 2014 International Conference on, 2014, pp. 1–6.

[21] N. Khamphakdee, N. Benjamas, and S. Saiyod, "Improving Intrusion Detection System based on Snort rules for network probe attack detection," presented at the Information and Communication Technology (ICoICT), 2014 2nd International Conference on, 2014, pp. 69–74.

[22] H. Holm, "Signature based intrusion detection for zero-day attacks:(not) a closed chapter?," presented at the 2014 47th Hawaii International Conference on System Sciences, 2014, pp. 4895–4904.

[23] B. M. Beigh and M. Peer, "Performance evaluation of different intrusion detection system: An empirical approach," presented at the Computer Communication and Informatics (ICCCI), 2014 International Conference on, 2014, pp. 1–7.

[24] R. Al-Dalky, K. Salah, H. Otrok, and M. Al-Qutayri, "Accelerating snort NIDS using NetFPGA-based Bloom filter," presented at the 2014 International Wireless Communications and Mobile Computing Conference (IWCMC), 2014, pp. 869–874.

[25] Z. Trabelsi and S. Zeidan, "IDS performance enhancement technique based on dynamic traffic awareness histograms," presented at the 2014 IEEE International Conference on Communications (ICC), 2014, pp. 975–980.

[26] Y. Xu, J. Jiang, R. Wei, Y. Song, and H. J. Chao, "TFA: A Tunable Finite Automaton for Pattern Matching in Network Intrusion Detection Systems," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 10, pp. 1810–1821, 2014.

[27] O. Al-Jarrah and A. Arafat, "Network Intrusion Detection System using attack behavior classification," presented at the Information and Communication Systems (ICICS), 2014 5th International Conference on, 2014, pp. 1–6.

[28] N. Dwivedi and A. Tripathi, "Event Correlation for Intrusion Detection Systems," presented at the Computational Intelligence & Communication Technology (CICT), 2015 IEEE International Conference on, 2015, pp. 133–139.

[29] N. Naik, "Fuzzy Inference Based Intrusion Detection System: FI-Snort," presented at the Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM), 2015 IEEE International Conference on, 2015, pp. 2062–2067.

[30] M. Kumar and M. Hanumanthappa, "Cloud based intrusion detection architecture for smartphones," presented at the Innovations in Information, Embedded and Communication Systems (ICIIECS), 2015 International Conference on, 2015, pp. 1–6.
[31] F. Hachmi, K. Boujenfa, and M. Limam, "A Three-Stage Process to Detect Outliers and False Positives Generated by Intrusion Detection Systems," presented at the Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM), 2015 IEEE International Conference on, 2015, pp. 1749–1755.
[32] T. Ping, "Application Research on Network Security Based on Feature Matching Technology," presented at the 2015 Seventh International Conference on Measuring Technology and Mechatronics Automation, 2015, pp. 202–205.
[33] M. Aldwairi and K. Al-Khamaiseh, "Exhaust: Optimizing Wu-Manber pattern matching for intrusion detection using Bloom filters," presented at the Web Applications and Networking (WSWAN), 2015 2nd World Symposium on, 2015, pp. 1–6.
[34] Z. Afzal and S. Lindskog, "Automated testing of IDS rules," presented at the Software Testing, Verification and Validation Workshops (ICSTW), 2015 IEEE Eighth International Conference on, 2015, pp. 1–2.
[35] W. Li, W. Meng, X. Luo, and L. F. Kwok, "MVPSys: Toward practical multi-view based false alarm reduction system in network intrusion detection," *Comput. Secur.*, vol. 60, pp. 177–192, 2016.
[36] W. Park and S. Ahn, "Performance Comparison and Detection Analysis in Snort and Suricata Environment," *Wirel. Pers. Commun.*, pp. 1–12, 2016.
[37] W. Bul'ajoul, A. James, and M. Pannu, "Improving network intrusion detection system performance through quality of service configuration and parallel technology," *J. Comput. Syst. Sci.*, vol. 81, no. 6, pp. 981–999, 2015.
[38] N. Khamphakdee, N. Benjamas, and S. Saiyod, "Improving Intrusion Detection System Based on Snort Rules for Network Probe Attacks Detection with Association Rules Technique of Data Mining," *J. ICT Res. Appl.*, vol. 8, no. 3, pp. 234–250, 2015.
[39] B. Li, J. Li, and L. Liu, "CloudMon: a resource-efficient IaaS cloud monitoring system based on networked intrusion detection system virtual appliances," *Concurr Comput Pr. Exper*, vol. 27, no. 8, pp. 1861–1885, 2015.
[40] W. El–Hajj, M. Al–Tamimi, and F. Aloul, "Real traffic logs creation for testing intrusion detection systems," *Wirel. Commun. Mob. Comput.*, vol. 15, no. 14, pp. 1851–1864, 2015.
[41] O. Erdem, "Tree-based string pattern matching on FPGAs," *Comput. Electr. Eng.*, vol. 49, pp. 117–133, 2016.
[42] D. Singh, D. Patel, B. Borisaniya, and C. Modi, "Collaborative IDS Framework for Cloud," *Int. J. Netw. Secur.*, vol. 18, no. 4, pp. 699–709, 2016.
[43] K. Lee and S. Yun, "Hybrid memory-efficient multimatch packet classification for NIDS," *Microprocess. Microsyst.*, vol. 39, no. 2, pp. 113–121, 2015.
[44] S. Alter, "Defining information systems as work systems: implications for the IS field," *Eur. J. Inf. Syst.*, vol. 17, no. 5, pp. 448–469, 2008.
[45] S. Rahmatian, "Transaction Processing Systems," *Encycl. Informatton Syst.*, vol. 4, 2003.

[46] B. Ives, S. Hamilton, and G. B. Davis, "A Framework for Research in Computer-Based Management Information Systems," *Manag. Sci.*, vol. 26, no. 9, pp. 910–934, Sep. 1980.
[47] J. P. Shim, M. Warkentin, J. F. Courtney, D. J. Power, R. Sharda, and C. Carlsson, "Past, present, and future of decision support technology," *Decis. Support Syst. Dir. Nest Decade*, vol. 33, no. 2, pp. 111–126, Jun. 2002.
[48] R. H. Sprague, "A Framework for the Development of Decision Support Systems," *MIS Q.*, vol. 4, no. 4, pp. 1–26, 1980.
[49] A. F. Lukasheh, R. L. Droste, and M. A. Warith, "Review of expert system (ES), geographic information system (GIS), decision support system (DSS), and their applications in landfill design and management," *Waste Manag. Res.*, vol. 19, no. 2, pp. 177–185, 2001.
[50] H. J. Watson, R. K. Rainer, and C. E. Koh, "Executive Information Systems: A Framework for Development and a Survey of Current Practices," *MIS Q.*, vol. 15, no. 1, pp. 13–30, 1991.
[51] B. Daya, "Network security: History, importance, and future," *Univ. Fla. Dep. Electr. Comput. Eng.*, 2013.
[52] P. Janson and R. Molva, "Security in open networks and distributed systems," *Comput.-Netw. Secur.*, vol. 22, no. 5, pp. 323–346, Oct. 1991.
[53] P. W. Dowd and J. T. McHenry, "Guest Editors' Introduction-Network Security: It's Time to Take It Seriously," *Computer*, vol. 31, no. 9, pp. 24–28, 1998.
[54] J. Jang-Jaccard and S. Nepal, "A survey of emerging threats in cybersecurity," *J. Comput. Syst. Sci.*, vol. 80, no. 5, pp. 973–993, 2014.
[55] AT&T, "AT&T Cybersecurity Insights : Decoding the Adversary," AT&T, Dallas, Texas, USA, Volume 1, Oct. 2015.
[56] Dell SonicWall, "Dell Security Annual Threat Report," Veol 1, Feb. 2016.
[57] Hewlett Packard Enterprise Security Research, "HPE Security Research Cyber Risk Report 2016," Hewlett Packard Enterprise Security Research, 2016.
[58] Verizon, "2016 Data Breach Investigations Report," Verizon, Apr. 2016.
[59] O. Adeyinka, "Internet Attack Methods and Internet Security Technology," in *2008 Second Asia International Conference on Modelling & Simulation (AMS)*, 2008, pp. 77–82.
[60] P. Garcia-Teodoro, J. Diaz-Verdejo, G. Maciá-Fernández, and E. Vázquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges," *Comput. Secur.*, vol. 28, no. 1, pp. 18–28, 2009.
[61] S. Noel, D. Wijesekera, and C. Youman, "Modern intrusion detection, data mining, and degrees of attack guilt," in *Applications of data mining in computer security*, Springer, 2002, pp. 1–31.
[62] A. Lazarevic, V. Kumar, and J. Srivastava, "Intrusion detection: A survey," in *Managing Cyber Threats*, Springer, 2005, pp. 19–78.
[63] S. Gunasekaran, "Comparison of network intrusion detection systems in cloud computing environment," presented at the Computer Communication and Informatics (ICCCI), 2012 International Conference on, 2012, pp. 1–6.
[64] A. Alhomoud, R. Munir, J. P. Disso, I. Awan, and A. Al-Dhelaan, "Performance evaluation study of intrusion detection systems," *Procedia Comput. Sci.*, vol. 5, pp. 173–180, 2011.
[65] A. H. Alqahtani and M. Iftikhar, "TCP/IP Attacks, Defenses and Security Tools," *Int. J. Sci. Mod. Eng. IJISME*, vol. 1, no. 10, 2013.

[66] M. Kacic, P. Hanacek, M. Henzl, and I. Homoliak, "A concept of behavioral reputation system in wireless networks," presented at the 2013 47th International Carnahan Conference on Security Technology (ICCST), 2013, pp. 1–5.

[67] J. Timofte, "Intrusion detection using open source tools," *Inform. Econ. J. XII*, vol. 2, pp. 75–80, 2008.

[68] G. Kurundkar, N. Naik, and S. Khamitkar, "Network intrusion detection using Snort," *Int. J. Eng. Res. Appl.*, vol. 2, no. 2, pp. 1288–1296, 2012.

[69] M. Roesch, "Snort: Lightweight Intrusion Detection for Networks.," presented at the LISA, 1999, vol. 99, pp. 229–238.

[70] K. Salah and A. Kahtani, "Performance evaluation comparison of Snort NIDS under Linux and Windows Server," *J. Netw. Comput. Appl.*, vol. 33, no. 1, pp. 6–15, 2010.

[71] M. Guimaraes and M. Murray, "Overview of intrusion detection and intrusion prevention," presented at the Proceedings of the 5th annual conference on Information security curriculum development, 2008, pp. 44–46.

[72] V. Kumar and O. P. Sangwan, "Signature based intrusion detection system using snort," *Int. J. Comput. Appl. Inf. Technol.*, vol. 1, no. 3, pp. 35–41, 2012.

[73] L. Etienne, "Malicious traffic detection in local networks with snort," 2009.

[74] N. Provos, "Honeyd-a virtual honeypot daemon," in *10th DFN-CERT Workshop, Hamburg, Germany*, 2003, vol. 2, p. 4.