Teler has detected quite well. Teler can detect what type of attack is being carried out on the server, what IP address is attacking, and the user agent used by the user and then sends the warning results in real-time to the Telegram bot with a time lag of not more than 3 seconds. Future research may be possible to develop more features at Teler, such as implementing a prevention function against future attacks by utilizing data generated by Teler. For example, it implements machine learning to automatically blacklist certain IPs that are detected trying to attack the server.

## REFERENCES


[1] BSSN, "BSSN'S Measure to Detect Cyberthreats," Jakarta, 2019. doi: 10.1017/CBO9781107415324.004.

[2] A. Gupta and L. Sen Sharma, "Detecting attacks in high-speed networks: Issues and solutions," *Inf. Secur. J.*, vol. 29, no. 2, pp. 51–61, 2020, doi: 10.1080/19393555.2020.1722296.

[3] M. Tabash, M. A. Allah, and B. Tawfik, "Intrusion detection model using naive bayes and deep learning technique," *Int. Arab J. Inf. Technol.*, vol. 17, no. 2, pp. 215–224, 2020, doi: 10.34028/iajit/17/2/9.

[4] S. Jose, D. Malathi, B. Reddy, and D. Jayaseeli, "A Survey on Anomaly Based Host Intrusion Detection System," *J. Phys. Conf. Ser.*, vol. 1000, no. 1, 2018, doi: 10.1088/1742-6596/1000/1/012049.

[5] A. H. Hambali and S. Nurmiati, "Implementasi Intrusion Detection System (IDS) Pada Keamanan PC Server Terhadap Serangan Flooding Data," *Sainstech J. Penelit. dan Pengkaj. Sains dan Teknol.*, vol. 28, no. 1, pp. 35–43, 2018, doi: 10.37277/stch.v28i1.267.

[6] D. Utomo, M. Sholeh, and A. Avorizano, "Membangun Sistem Mobile Monitoring Keamanan Web Aplikasi Menggunakan Suricata dan Bot Telegram Channel," *Semin. Nas. Teknoka*, vol. 2, no. 2502, pp. 1–7, 2017.

[7] K. Ma, R. Jiang, D. Mianxiong, Y. Jia, and A. Li, "Neural Network Based Web Log Analysis for Web Intrusion Detection," *Springer Int. Publ.*, pp. 194–204, 2017, doi: 10.1007/978-3-319-72395-2.

[8] D. Siswanto, "Teler Real-time HTTP Intrusion Detection," 2020. https://github.com/kitabisa/teler (accessed Dec. 05, 2020).

[9] M. Baş Seyyar, F. Ö. Çatak, and E. Gül, "Detection of attack-targeted scans from the Apache HTTP Server access logs," *Applied Computing and Informatics*, vol. 14, no. 1. Elsevier B.V., pp. 28–36, Jan. 01, 2018, doi: 10.1016/j.aci.2017.04.002.

[10] A. Erlansari, F. F. Coastera, and A. Husamudin, "Early Intrusion Detection System (IDS) using Snort and Telegram approach," *Sisforma*, vol. 7, no. 1, p. 21, 2020, doi: 10.24167/sisforma.v7i1.2629.

[11] S. Suroto, "A Review of Defense Against Slow HTTP Attack," *JOIV Int. J. Informatics Vis.*, vol. 1, no. 4, p. 127, 2017, doi: 10.30630/joiv.1.4.51.

[12] R. S. Devi and M. M. Kumar, "Testing for Security Weakness of Web Applications using Ethical Hacking," no. Icoei, pp. 354–361, 2020.

[13] J. C. de Oliveira, D. H. Santos, and M. ́ario P. Neto, "Chatting with Arduino Platformthrough Telegram Bot," in *2016 IEEE International Symposium on Consumer Electronics*, 2016, pp. 1–2.

[14] K. Coffey, R. Smith, L. Maglaras, and H. Janicke, "Vulnerability Analysis of Network Scanning on SCADA Systems," *Secur. Commun. Networks*, vol. 2018, 2018, doi: 10.1155/2018/3794603.

[15] A. A. Kristanto, Y. Harjoseputro, and J. E. Samodra, "Implementasi Golang dan New Simple Queue pada Sistem Sandbox Pihak Ketiga Berbasis REST API," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 4, no. 4, pp. 745–750, 2020.

[16] M. Barthelmäs, M. Killinger, and J. Keller, "Using a Telegram chatbot as cost-effective software infrastructure for ambulatory assessment studies with iOS and Android devices," *Behav. Res. Methods*, 2020, doi: 10.3758/s13428-020-01475-4.

[17] F. Holik and S. Neradova, "Vulnerabilities of modern web applications," *2017 40th Int. Conv. Inf. Commun. Technol. Electron. Microelectron. MIPRO 2017 - Proc.*, pp. 1256–1261, 2017, doi: 10.23919/MIPRO.2017.7973616.

[18] S. K. Paudel, "Vulnerable Web Applications and How To Audit Them," Oulu University of Applied Sciences, 2016.

[19] G. C. Deka, *NoSQL Web Crawler Application*, 1st ed., vol. 109. Elsevier Inc., 2018.

[20] Sucurisecurity, "Directory Guessing Brute Force Attacks," 2019. https://docs.sucuri.net/definitions/attacks/brute-force/directory-guessing-brute-force-attacks/ (accessed Dec. 12, 2020).