Identifying Security Threats in the System Using Automated Security Logs

Publisher: IEEE Cite This PDF

Yadidiah Kanaparthi ; Tamer Mohamed Abdellatif ; Ahmed Ali Seyam ; Gandeva Bayu Satrya **All Authors**

Abstract:
Security Logs play a crucial role in detecting and monitoring security threats while authenticating a user in a network. This paper emphasizes various vulnerabilities, like the increasing complexity of authentication systems and employees logging from their devices. Tools like Syslog-ng and iptables were used in a Kali Linux environment to generate automated security incident detection using logs. Several tests like failed login, unauthorized access, Denial of Service (DOS), and SQL Injection attempts were conducted to assess the security of the login page. The machine learning algorithm, Isolation Forest was employed for anomaly detection, which identifies rare patterns by isolating data points that deviate from typical behavior. This unsupervised learning algorithm constructs trees that split recursively to isolate anomalies in the dataset to effectively isolate anomalies to enhance log analysis and enable real-time identification of potential threats. During a DoS attack, the server's filtering mechanisms prevented the logging of redundant requests, resulting in 12,612 recorded login attempts out of 20,000 detected requests. Isolation Forest-based anomaly detection, using a test size of 35% and a contamination rate of 0.1, identified a low anomaly rate with consistent scores between the training (0.0007) and test sets (0.0008), indicating effective anomaly detection and log storage processes.

Published in: 2024 Third International Conference on Sustainable Mobility Applications, Renewables and Technology (SMART)

Date of Conference: 22-24 November 2024

DOI: 10.1109/SMART63170.2024.10815284

Date Added to IEEE *Xplore*: 31 December 2024

Publisher: IEEE

ISBN Information:

Conference Location: Dubai, United Arab Emirates

Back to Results