

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](#)

106
Full
Text Views

Abstract
Document Sections
I. Introduction
II. Literature Review
III. Methodology
IV. Results
V. Conclusion
Authors
Figures
References
Keywords
Metrics
More Like This

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

Sign in to Continue Reading

Authors	▼
Figures	▼
References	▼
Keywords	▼
Metrics	▼



[Back to Results](#)



IEEE Personal Account

[CHANGE USERNAME/
PASSWORD](#)

Purchase Details

[PAYMENT OPTIONS](#)
[VIEW PURCHASED
DOCUMENTS](#)

Profile Information

[COMMUNICATIONS
PREFERENCES](#)
[PROFESSION AND
EDUCATION](#)
[TECHNICAL INTERESTS](#)

Need Help?

[US & CANADA: +1 800
678 4333](#)
[WORLDWIDE: +1 732
981 0060](#)
[CONTACT & SUPPORT](#)

Follow

[f](#) [@](#) [in](#) [v](#)



[About IEEE Xplore](#) | [Contact Us](#) | [Help](#) | [Accessibility](#) | [Terms of Use](#) | [Nondiscrimination Policy](#) | [IEEE Ethics Reporting](#) | [Sitemap](#) |

[IEEE Privacy Policy](#)

A public charity, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.

© Copyright 2025 IEEE - All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies.

