Initial Post

Initial Post

by Lauren Pechey - Thursday, 10 July 2025, 11:33 AM

The Importance of Logging for Security

Logging plays a critical role in modern network security management (NSM) and forensic analysis (FA). Berger (2023) highlights how comprehensive logging enables security analysts to detect anomalies, trace breaches, and meet compliance requirements. Similarly, Nyangaresi et al. (2024) argue that without systematic logging, organisations lack the visibility needed to identify threats and respond effectively.

Benefits and Risks of Effective Log Management

A well-designed logging system can detect brute force attempts, unusual access patterns, insider threats, and other suspicious activities. For example, Shang et al. (2021) emphasise that log management is fundamental to incident detection and response frameworks. Logs provide evidence trails for post-incident investigations and can support legal action if breaches occur (Ahmed et al., 2020).

However, logs themselves can become targets. Attackers can exploit misconfigured or weakly secured logging systems to cover their tracks by deleting or altering log entries. As Nyangaresi et al. (2024) caution, if logs are not encrypted, attackers can extract sensitive information, including credentials or system details, which can escalate the impact of a breach. Log injection attacks are also possible if inputs are not properly sanitised (Shang et al., 2021).

Best Practices for Secure Logging

To balance these concerns, organisations should implement secure log management practices, such as encryption, strict access controls, regular audits, and offsite or immutable logging solutions (Ahmed et al., 2020). Additionally, using security information and event management (SIEM) tools can help automate anomaly detection while securing logs (Berger, 2023).

In summary, while logging is indispensable for security monitoring and analysis, its implementation must be robust to prevent it from becoming a new attack vector. As Berger (2023) and Nyangaresi et al. (2024) emphasise, organisations must strike a balance between collecting actionable data and protecting it against misuse.

References

Ahmed, F., Jahangir, U., Rahim, H., Ali, K., & Agha, D.-e.-S. (2020) 'Centralized log management using Elasticsearch, Logstash and Kibana', *2020 International Conference on Information Science and Communication Technology (ICISCT)*, Karachi, Pakistan, 27–28 November. IEEE, pp. 1–7.

Berger, J. (2023) What is Log4Shell? The Log4j vulnerability explained (and what to do about it), *Dynatrace News*. Available at: **https://www.dynatrace.com/news/blog/what-is-log4shell/** (Accessed: 6 July 2025).

Li, H., Shang, W., Adams, B., Sayagh, W., & Hassan, A. (2021) 'A qualitative study of the benefits and costs of logging from developers' perspectives', *IEEE Transactions on Software Engineering*, 47(12), pp. 2858–2873. **https://doi.org/10.1109/TSE.2020.2970422**

Nyangaresi, V. O., Alsolami, E., & Ahmad, M. (2024) 'Trust-enabled energy efficient protocol for secure remote sensing in supply chain management', *IEEE Access*, 12(1), pp. 113553–113564. **https://doi.org/10.1109/ACCESS.2024.3442619**

Maximum rating: - Permalink Reply