Network Security - Module 3

The Pros and Cons of logging - The impact of Log4j

Collaborative Discussion 2

Summary Post

While observing recent activities involving log4j and common vulnerability exploits associated with it, It has become clear that emphasis needs to be placed on good log management planning, implementation and monitoring if we are to be able to detect and respond quickly to vulnerabilities and exploits within the systems used and for forensic investigations.
However, it appears that there are many challenges for logging, such as ensuring the protection of their confidentiality and integrity (Kent & Souppaya, 2006).

Open-source software is available to help businesses with logging, such as Nagios and Snort. But, open source software can also create challenges.Those challenges can be easier understood and mitigated via software having been registered into an SBOM. SBOM is a software bill of rights that allows automated identification of vulnerabilities and exploits of the various softwares that are used to develop a product (Enisa, 2023:33).

Alternatively, a Software Composition Analysis (SCA) tool scans open source software for potential vulnerabilities but does it passively, it does not execute the software (Enisa 2023:26). This automation tool is also able to create an SBOM for inspections at a later date (Enisa 2023:34), which may help in identifying and mitigating exploits such as Log4j quicker.

This topic surrounding the importance of logging and the issues highlighted by the log4j exploit has been covered in-depth throughout this discussion.
However, as businesses transition to the cloud, we have to also understand the complications and vulnerabilities surrounding on-premise/off-premise logging. logs could be spread over several data centers and cross into different areas of compliance and regulations (Mell et al, 2016). Attackers can also delete logs to cover their tracks and create difficulties during digital forensic investigations. An option may be to ensure that “LogRotate” is set-up to allow log forwarding via TCP to a secure syslog machine for log storage.

References

Enisa (2023) Developing national vulnerability programmes. Available at: https://www.enisa.europa.eu/publications/developing-national-vulnerabilities-programmes. [Accessed on 23rd February 2023]

Kent, K & Souppaya, M. (2006) Guide to computer security log management. NIST 800-92. Available from: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf [Accessed on 17th February 2023]

P. Mell , S. Gavrila & J. Shook (2016) Restricting Insider Access through Efficient Implementation of Multi-Policy Access Control Systems. *MIST ‘16: Proceedings of the 8th ACM CCS International Workshop on Managing Insider Security Threats*, Vienna, Austria, October 24-28; 13-22.