Network Security - Module 3

The Pros and Cons of logging - The impact of Log4j

Collaborative Discussion 2

Peer response

My Peer response to Michael (A student)

Michael, you have assimilated these points rather well and it was interesting to read your collection of findings regarding logging system information. One of your findings has mentioned non-repudiation, which is often forgotten with the triad of confidentiality, integrity and availability.

You have suggested that organizations should “Encrypt stored logs”, this is a really important suggestion and one is supported by NIST (2006), who state that “Organizations should store logs for compliance and regulation laws” because of the requirement to comply with regulations and standards such as PCI-DSS and ISO27001 (Zeng et al 2016). Possibly, something that may help your suggestion is a common type of security software for computer security log data which can be network or host based authentication servers that help log each authentication attempt (NIST, 2006).

Do you think that logging management is the way forward to be able to log the categories of logs and link them to their individual purpose?
An example being: category - system/application/data changes > Purpose: monitoring for changes to expose system attacks.

To conclude, I really enjoyed reading your approach to this topic. It has become evident that the integrity of logs needs to be maintained and checked due to exploits such as log4j 2 which took place. The ability for logs to be changed after recording computer or network system activity is worrying and could become an expensive issue for businesses.

References

NIST. (2006) Guide to computer security log management: *NIST 800-92.* Available from: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf [Accessed on 14th February 2023]

Zeng, L., Xiao, Y., Chen, H., Sun, B. and Han, W., (2016). Computer operating system logging and security issues: a survey. *Security and communication networks*, *9*(17), pp.4804-4821.