Network Security - Module 3

The Pros and Cons of logging - The impact of Log4j

Collaborative Discussion 2

Peer response

My Peer response to Antonios (A student)

Antonios, this was a nice discussion to read and I found it thought inspiring, especially the section where you provided some possible solutions to reduce risk in logging. It seems that logging is here to stay. Zeng et al (2016) has stated that the process of logging in operating systems has become a crucial element of their respective kernels, but it comes with its challenges.

According to NIST (2006), log data analysis is the most important aspect of log management but also the most challenging, which could also mean that the inability to analyze logs correctly or promptly has, in itself, become a security risk. This risk was also obvious to the adversaries who exploited the apache servers log4j.

To reduce risk, you suggested using several approaches such as implementing intrusion detection systems (IDS), the use of MD5 or SSH integrity protection and integrity, and TLS protocol so that the confidentiality of the logs messages remain intact.

Another mitigation available for log4j 2.x that solved infinite recursion issue is in the code itself, Apache software foundation had shared a fix that says “In PatternLayout in the logging configuration, replace Context Lookups like ${ctx:loginId} or $${ctx:loginId} with Thread Context Map patterns (%X, %mdc, or %MDC)” for example.

To conclude, Berger (2021) has explained that log4j also affects consumers and that consumers should disconnect their smart home equipment until the manufactures have patched the vulnerability. This is extremely worrying when we consider that the average person would not know about this advice and would therefore be vulnerable.

References

Apache software foundation (2021). Security mitigation for log4j. Available from: https://logging.apache.org/log4j/2.x/security.html [Accessed on 16th February 2023]

Berger, A. (2021) What is Log4hell? The Log4j vulnerability explained (and what to do about it). Available from: https://www.dynatrace.com/news/blog/what-is-log4shell/?utm_source=google&utm_medium=cpc&utm_term=log4j%20vulnerability%20explained&utm_campaign=uk-application-security&utm_content=none&gclid=CjwKCAjwiuuRBhBvEiwAFXKaNJd3hLzYlujXuVbTIP63_IioBFvzAYOePxfft2D6ded7EXfaTu4j4BoCrHAQAvD_BwE&gclsrc=aw.ds [Accessed 14 February 2023].

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.