Unit 9: System Logging and Forensics

Objectives:

- Review the types of logs and tools used to view logs.
- Explore different types of logging and analysis tools.
- Describe the steps involved in a security breach response.
- List a number of tools used for forensic investigations.

Outcomes:

- Explain how and why logging is used in security systems.
- Describe which tools to use for logging and analysis.
- Explain how logging is used in incident investigations.
- Describe the best forensic techniques to use.

Reflection:

Digital evidence can occur in many ways. Examples include surfing histories, chat logs, log-in files, and deleted files or images. It is vital to maintain track of what the client, programs, and software platforms are doing. Forensics experts view these data as a critical component of the investigation's digital evidence (Studiawan, Sohel and Payne, 2019).

As a protective measure, a log serves as a warning sign if something is amiss. Frequently checking log may help you to discover suspicious activity on your computer. Using system logs, you can learn about potential security dangers to your system and take action to prevent them. In most cases, you can depend on your computer to get information on network connections.Out-of-memory exceptions and hard drive faults can be found in log data. Our team will be able to identify the "why" behind any issues brought to our attention by users or that we have discovered ourselves (Tunis, 2019).

A system log is a collection of data that enables you spot problems before they become risks to your system. On most cases, your device collects data that exposes what is going on in your environment (Noura et al., 2020).

In contrast to cyber security, digital forensics is centered on restoration and response. Data, applications, networking as well as other technology infrastructure are all protected by both.

The fundamental steps Computer-related data for vulnerability assessment prevention or crime, fraudulent, espionage, or police inquiries should be collected, processed and preserved. Nowadays, DNA testing and analysis is regarded a most trustworthy of all the forensic technologies available to law enforcement (Pichan, A., Lazarescu, M. and Soh, S.T. (2018))

References

Noura, H.N., Salman, O., Chehab, A. and Couturier, R. (2020). DistLog: A distributed logging scheme for IoT forensics. *Ad Hoc Networks*, 98, p.102061. doi:10.1016/j.adhoc.2019.102061.

Pichan, A., Lazarescu, M. and Soh, S.T. (2018). Towards a practical cloud forensics logging framework. *Journal of Information Security and Applications*, [online] 42, pp.18–28. doi:10.1016/j.jisa.2018.07.008.

Studiawan, H., Sohel, F. and Payne, C. (2019). A survey on forensic investigation of operating system logs. *Digital Investigation*, 29, pp.1–20. doi:10.1016/j.diin.2019.02.005.

Tunis, J. (2019). *Logging and Monitoring: Why You Need Both*. [online] The New Stack. Available at: https://thenewstack.io/logging-and-monitoring-why-you-need-both/.