Exercise 3

24/08/2021

Event log analysis

1) Event Viewer

It is an important component of Microsoft's Windows family of operating systems. It lets administrators and users view event logs on a local or remote machine. Applications and operating-system components can use this centralized log service to report events that have taken place, such as a failure to start a component or to complete an action. Event Viewer uses event IDs to define the uniquely identifiable events that a Windows computer can encounter. Event logs record events taking place in the execution of a system in order to provide an audit trail that can be used to understand the activity of the system and to diagnose problems. It is often useful to combine log file entries from several sources. This approach, in combination with statistical analysis, may yield correlations between seemingly unrelated events on different servers. Other solutions employ network-wide querying and reporting. Windows Event Logs can potentially be used by a forensic examiner to show what a user has done on a computer. They can be used to assist in answering the question "could this happen?"

Refer the following links for more details about the use of event logs for forensics

https://en.wikipedia.org/wiki/Event_Viewer

https://www.blackbagtech.com/blog/2017/01/27/leveraging-windows-event-logs-in-examinations/

https://isc.sans.edu/forums/diary/Windows+Events+log+for+IRForensics+Part+1/21493/

https://medium.com/@lucideus/introduction-to-event-log-analysis-part-1-windows-forensics-manual-2018-b936a1a35d8a

https://medium.com/@lucideus/event-log-analysis-part-2-windows-forensics-manual-2018-75710851e323

Event ids are generated for events useful in forensic investigation. Examples include

a) Successful logon

b) Failed login

c) A new user account was created

Use the Event Viewer tool in a Microsoft Windows computer and take screenshots of **THREE** security related events such as

(i) Logon

(ii) Logoff

(iii) Attempt made to query the existence of a blank password for an account

2) The Event Log Explorer tool

This tool can be got from https://eventlogxp.com it is available for free for personal non-commercial use. It is also available for commercial use. It is an extension of the Microsoft Event Viewer tool. It has many features helpful in forensic analysis. https://eventlogxp.com/event-log-forensic.html

Download this tool on a Windows computer and take screenshots of **two security related events** such as those listed in the previous exercise.