Lab Assignment

Cybersecurity Professional Program

Digital Forensics Incident Response

Log Analysis

DFIR-09-L1
Event Viewer Investigation

Lab Objective

Understand Event Viewer logs and how to filter events for better results. The lab will help learners practice filtering and working with event IDs that can help during investigations.

Lab Mission

Use the event IDs to help search for events and learn about their structure.

Lab Duration

10–15 minutes

Requirements

- Knowledge of event log filtering and structure

Resources

- Environment & Tools
  - Windows VM
  - Text editor
- Extra Lab Files
  - ***Security.evtx***

Lab Task: Windows Investigation

1. Transfer the ***Security.evtx*** file to the Windows VM and double-click to open via Event Viewer.
2. In the imported security logs, search for the names of three new users with the use of filtering event IDs.
   Can you tell who was responsible for the creation of the users?
3. One user was disabled. Can you tell what the name of that user is?
4. A brute-force attack can be viewed in ***Security.evtx***. Can you investigate which user and IP were under attack and if the brute-force was successful?
5. Users were added to the Administrators group. Which users and who added them?
6. The security log was cleared. Can you tell who cleared it?
7. Which new groups were created and by whom?
8. Which user was deleted and by whom?