LAB6

Scenario

PurpleHawkS R&D Manager came across compromised system logs, and he wanted Security Developer to review the device logs and create a sigma rule.

Compromised System Raw Log -

Log added to GitHub - purplehawks_suspicious_rawlog.txt

Exercise

As a Security Developer, review logs and write sigma rule so that it can be detected.

Requirements:

1. Write a sigma rule
2. Continue with LAB8 to test the detection