LAB4

Scenario

PurpleHawkS TI Manager came across a few TTPs, and he wanted Threat Intel Analyst to emulate the adversary's actions and review the device logs to provide the details to the detection team.

Adversary Emulation TTPs

- Dump LSASS.exe Memory using comsvcs.dll (T1003.001)
- Create Hidden User in Registry (T1564.002)
- Enumerate all accounts on Windows (Local) (T1087.001)
- PowerShell Command Execution (T1059.001)
- Create a new Windows admin user (T1136.001)

Exercise

As a Threat Intel Analyst, emulate adversaries and review all TTPs information on the windows device.

Requirements:

1. Review processes in “Process-Hacker” for each step.
2. Run caldera-agent on Windows-10/11 device.
3. Create an OPERATIONS in Caldera (Please note: even if its shows failed the log is still created)
4. Emulate adversary TTPs (listed above).
5. Review sysmon/security logs in “Event-Viewer”.
6. Review sysmon logs in “Sysmon-View”.