LAB10

Scenario

Conduct a purple teaming exercise on the knowledge collected with all of the PurpleHawkS LABs by using ATTPwn. This is preloaded adversary emulations similar to Caldera.

Exercise

As a Security Engineer/Analyst, follow the purple teaming runbook by using any tool of your choice and using ATTPwn as Emulation.
Please Note: This tool has not been updated for the past 4 years so it would be better for lab purposes.

Requirements:

1. Create your own scenario with TTPs loaded in the ATTPwn tool.
2. Red Team - Emulation TTP using ATTPwn.
3. Purple Team - Exercise details on DETT&CT or VECTR.
4. Export the logs from the Windows device.
5. Review sysmon logs in “Sysmon-View”.
6. Detection Engineering - Add/Create detections.
7. Blue Team - Run the logs with Threathound or Zircolite.