LAB8

Scenario

PurpleHawkS R&D Manager was given an emulation report, and he wanted Security Developer to review detection miss, create a new rule and run detection tool to identify alerts.

Compromised System

Log file is added to GitHub - PurpleHawkS-ThreatHound_Detection_Windows_Logs.evtx

Current Detection is added to GitHub - Please use cmd “mkdir” and add the rules to $PATH/ThreatHound/rules

- purplehawks_procdump_execution.yml
- purplehawks_psexec_remote_execution.yml

Exercise

As a Security Developer, review current detection, add new sigma rule which was not detection and run ThreatHound detection tool to identify that current/new rule is detected.

Requirements:

1. Run the ThreatHound tool against the log file.
2. LAB6 sigma rule and add to $PATH/ThreatHound/rules.
3. Run the ThreatHound tool to test the detection.
4. Refine the rules if not matching and repeat point 3 until all rules are matched.

Please Note: All three rules should match. Please review the logs for refining the rules.