Powershell Logging Mechanisms

Powershell Log Sources

Powershell Logging Module

- Module Block
  - Presented with PsV3
  - Windows Powershell.evtx
    - EID 800
    - EID 400 & 403
      - Beginning and End of Session
- Script Block
  - -Presented with PsV5
    -Not Enabled By Default
    -If Suspicious situation exist, logging started automaticly
    -All usage of powershell logged
  - Microsoft-Windows-PowerShellOperational.evtx
    - 4103
    - 4104
    - 4105
    - 4106

Transcripts

- Presented with PsV4
  Not enabled by default
- C:\Users\"USERNAME"\Documents

PsReadline_ConsoleHost_history.txt

- PsV5-Win10 Enabled by Default
- 4096 Command
- %userprofile%\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_history.txt

Event Log - WinRM

- Microsoft-Windows-WinRM%4Operational.evtx
  - EID 6 — When Client tries to access anywhere via PSRemote | Created on Client.
  - EID 169 — When someone triest to access target via PSRemote | Created on Target