Core Windows Processes

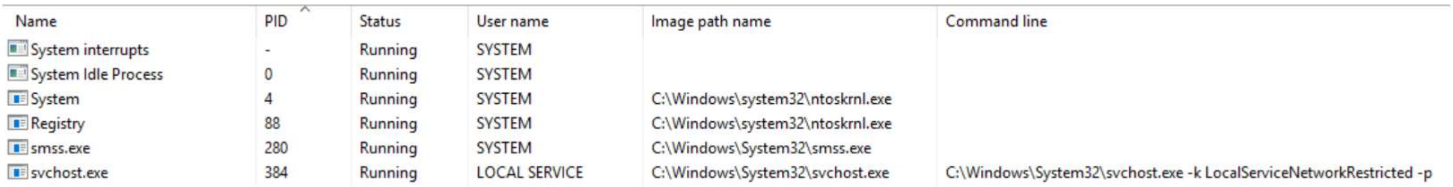
Task Manager

- built in GUI based Windows utility that allows users to see what is running on the Windows system
- provides information on resource usage, such as how much each process utilizes CPU and memory

Task Manager columns:

Type – each process falls into 1 of 3 categories (Apps, Background process, or Windows process)
Publisher – name of the program/file
PID – process identifier number. Windows assigns a unique process identifier each time a program starts
Process Name – file name of the process
CPU – amount of CPU (processing power) the process uses
Memory – amount of physical working memory utilized by the process

*Good columns to add are 'Image path name' and 'Command line'
- these 2 columns can quickly alert an analyst of any outliners with a given process



Name	PID	Status	User name	Image path name	Command line
System interrupts	-	Running	SYSTEM		
System Idle Process	0	Running	SYSTEM		
System	4	Running	SYSTEM	C:\Windows\system32\ntoskrnl.exe	
Registry	88	Running	SYSTEM	C:\Windows\system32\ntoskrnl.exe	
smss.exe	280	Running	SYSTEM	C:\Windows\System32\smss.exe	
svchost.exe	384	Running	LOCAL SERVICE	C:\Windows\System32\svchost.exe	C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p

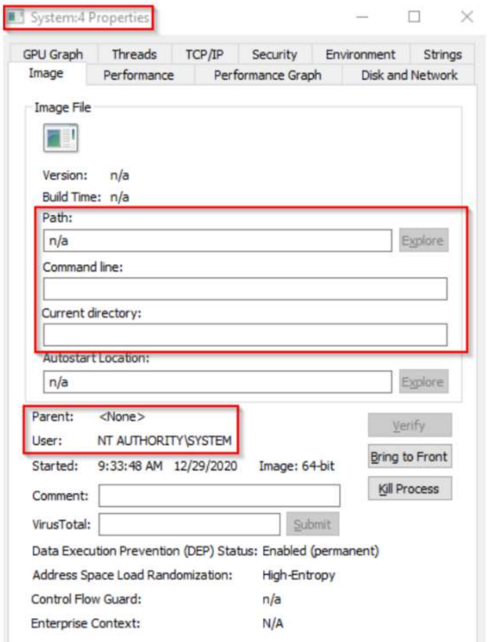
PID 384 is paired with a process name svchost.exe, but if the Image path name + Command line is not what it's expected to be, then we can investigate.

Tools: Process Hacker + Process Explorer to obtain more information about each Windows process.

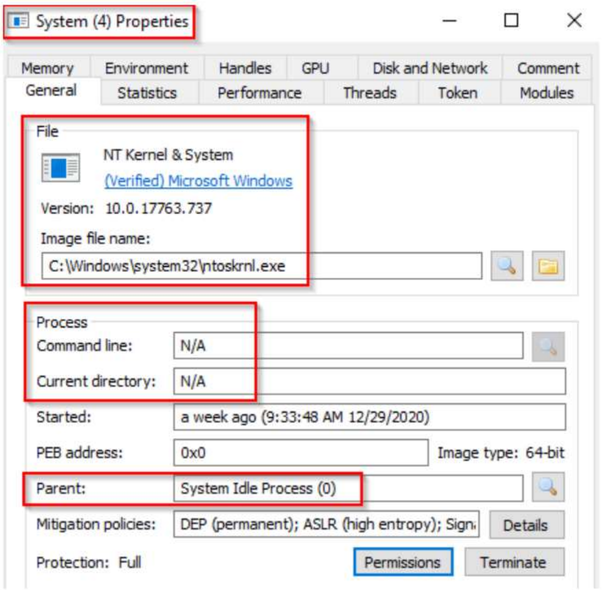
System

- first Windows process on the list is System
- PID for System is always 4

Use Process Explorer + Process Hacker to view properties



Version: n/a
Build Time: n/a
Path: n/a
Command line:
Current directory:
Autostart Location: n/a
Parent: <None>
User: NT AUTHORITY\SYSTEM
Started: 9:33:48 AM 12/29/2020 Image: 64-bit
Comment:
VirusTotal:
Data Execution Prevention (DEP) Status: Enabled (permanent)
Address Space Load Randomization: High-Entropy
Control Flow Guard: n/a
Enterprise Context: N/A



NT Kernel & System
(Verified) Microsoft Windows
Version: 10.0.17763.737
Image file name: C:\Windows\system32\ntoskrnl.exe
Command line: N/A
Current directory: N/A
Started: a week ago (9:33:48 AM 12/29/2020)
PEB address: 0x0 Image type: 64-bit
Parent: System Idle Process (0)
Mitigation policies: DEP (permanent); ASLR (high entropy); Sign
Protection: Full