1 - System

Task 3 System

The first Windows process on the list is **System**. It was mentioned in a previous section that a PID for any given process is assigned at random, but that is not the case for the System process. The PID for System is always 4. What does this process do exactly?

The official definition from Windows Internals 6th Edition:

"The System process (process ID 4) is the home for a special kind of thread that runs only in kernel mode a kernel-mode system thread. System threads have all the attributes and contexts of regular user-mode threads (such as a hardware context, priority, and so on) but are different in that they run only in kernel-mode executing code loaded in system space, whether that is in Ntoskrnl.exe or in any other loaded device driver. In addition, system threads don't have a user process address space and hence must allocate any dynamic storage from operating system memory heaps, such as a paged or nonpaged pool."

What is user mode? Kernel-mode? Visit the following link to understand each of these.

Now, what is normal behaviour for this process? Let's use Process Explorer and view the properties of the System.

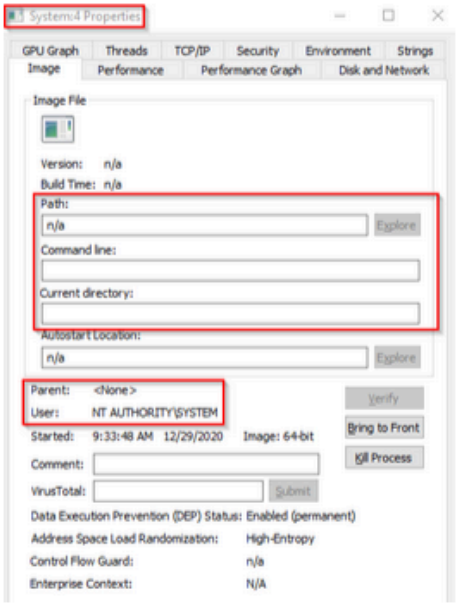
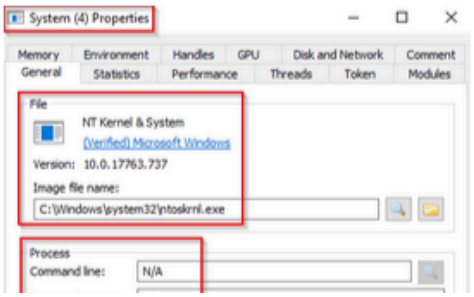


Image Path: N/A
Parent Process: None
Number of Instances: One
User Account: Local System
Start Time: At boot time

The information is slightly different if we view the System properties using Process Hacker.



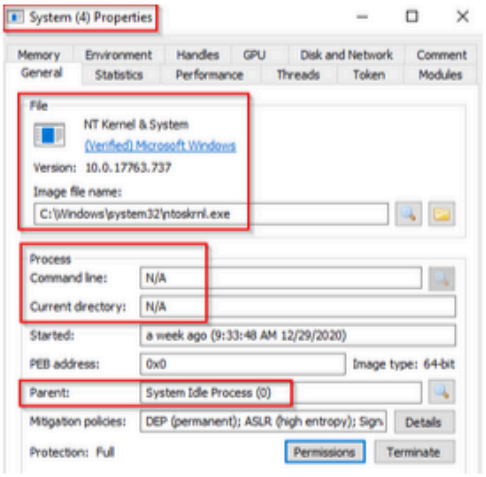


Image Path: C:\Windows\system32\ntoskrnl.exe (NT OS Kernel)
Parent Process: System Idle Process (0)

Technically this is correct. You may notice that Process Hacker confirms this is legit (Verified) Microsoft Windows.

What is unusual behaviour for this process?

- A parent process (aside from System Idle Process (0))
- Multiple instances of System. (Should only be one instance)
- A different PID. (Remember that the PID will always be PID 4)
- Not running in Session 0

Answer the questions below

What PID should System always be?

0

Submit