9 - explorer.exe

Task 11 explorer.exe

The last process we'll look at is **Windows Explorer**, **explorer.exe**. This process gives the user access to their folders and files. It also provides functionality for other features, such as the Start Menu and Taskbar.

As mentioned previously, the Winlogon process runs userinit.exe, which launches the value in `HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell`. Userinit.exe exits after spawning explorer.exe. Because of this, the parent process is non-existent.

There will be many child processes for explorer.exe.

explorer.exe	4040	WIN-1O0UJBNP9G7\Administrator	Windows Explorer	C:\Windows\explorer.exe	C:\Windows\Explorer.EXE
vm3dservice.exe	4552	WIN-1O0UJBNP9G7\Administrator	VMware SVGA Helper Service	C:\Windows\System32\vm3dservice.exe	"C:\Windows\System32\vm3dservice.exe" -u
vmtoolsd.exe	4588	WIN-1O0UJBNP9G7\Administrator	VMware Tools Core Service	C:\Program Files\VMw...\vmtoolsd.exe	"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmusr
ProcessHacker.exe	5008	WIN-1O0UJBNP9G7\Administrator	Process Hacker	C:\Program Files\...\ProcessHacker.exe	"C:\Program Files\Process Hacker 2\ProcessHacker.exe"
cmd.exe	3308	WIN-1O0UJBNP9G7\Administrator	Windows Command Processor	C:\Windows\System32\cmd.exe	"C:\Windows\system32\cmd.exe"
conhost.exe	4940	WIN-1O0UJBNP9G7\Administrator	Console Window Host	C:\Windows\System32\conhost.exe	\??\C:\Windows\system32\conhost.exe 0x4
regedit.exe	2636	WIN-1O0UJBNP9G7\Administrator	Registry Editor	C:\Windows\regedit.exe	regedit
procexp64.exe	1156	WIN-1O0UJBNP9G7\Administrator	Sysinternals Process Explorer	C:\Users\Administrato...\procexp64.exe	"C:\Users\Administrator\Desktop\ProcessExplorer\procexp64.exe"
Taskmgr.exe	3556	WIN-1O0UJBNP9G7\Administrator	Task Manager	C:\Windows\System32\Taskmgr.exe	"C:\Windows\system32\taskmgr.exe" /4

What is normal?

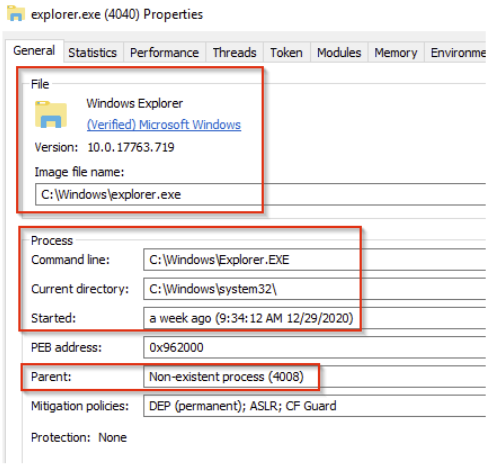
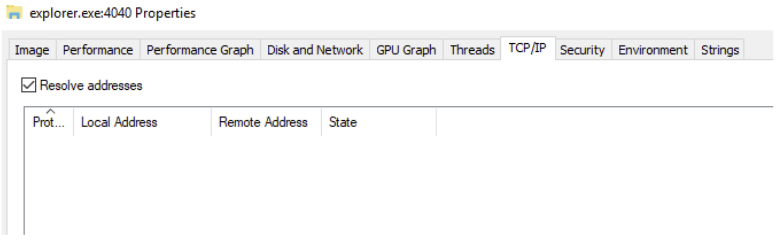


Image Path: %SystemRoot%\explorer.exe
Parent Process: Created by userinit.exe and exits
Number of Instances: One or more per interactively logged-in user
User Account: Logged-in user(s)
Start Time: First instance when the first interactive user logon session begins

What is unusual?

- An actual parent process. (userinit.exe calls this process and exits)
- Image file path other than C:\Windows
- Running as an unknown user
- Subtle misspellings to hide rogue processes in plain sight
- Outbound TCP/IP connections



Note: The above image is the explorer.exe properties view from Process Explorer.

Answer the questions below

What is the non-existent process for explorer.exe?

userinit.exe ✓ Correct Answer