1. **Begin your work by thoroughly exploring and collecting fundamental details about the system in question. It's critical to identify which operating system is in use, understand the hardware configuration, review the currently running processes, catalog all user accounts, and clarify what security mechanisms are active. This comprehensive initial investigation, often referred to as creating a system inventory, forms the foundation for any further analysis or troubleshooting. Skipping this step is like navigating without a map: you lose visibility into the environment's normal state, making it much harder to detect anomalies, diagnose problems, or accurately assess the system's overall security posture.**

```
PS C:\WINDOWS\system32> Get-Process
>>

Handles  NPM(K)    PM(K)      WS(K)     CPU(s)      Id  SI ProcessName
-------  ------    -----      -----     ------      --  -- -----------
    162       8     2676       8820       2.13    7768   0 AggregatorHost
    497      30    19992      33208       0.95    9688   4 ApplicationFrameHost
    205      12     7420      13140       1.14   55116   0 audiodg
    197      12     2780      10972       0.22    9932   4 AutoModeDetect
   1553      65   660264     288608     268.89   90244   4 AyuGram
    551      39    57616       2080       0.22   17048   4 CalculatorApp
    226      16    10604      20168       0.63    3452   4 chrome
    560      48   608264     510040     372.11    5584   4 chrome
   2733     102   269268     365372     211.17    8180   4 chrome
    322      11     6984       9260       0.08   10916   4 chrome
    338      27    51424     109844       1.23   11916   4 chrome
    336      22    14632      24716      13.50   11976   4 chrome
    216      19    13176      29296       0.06   14676   4 chrome
    467      36    30720      57172      38.72   15448   4 chrome
    539      27    67460      38920       0.48   16204   4 chrome
    417      32    72768     131196       2.03   18612   4 chrome
    524      43   259260     307864      48.95   19288   4 chrome
    403      31   541928     217132      25.34   55252   4 chrome
    263      25    61244      87780      11.63   67112   4 chrome
    505      45   362232     470736      20.66   70472   4 chrome
    514      50   268812     311284      24.08   75788   4 chrome
    468      52   341408     341528     101.66   78948   4 chrome
    310      27    50672      90364       8.06   82876   4 chrome
    375      36   186852     202852      11.28   84908   4 chrome
    978      48   249676     289840       8.72   85768   4 chrome
    530      49   267796     285184      17.17   86688   4 chrome
    564      57   373924     443956       8.11   88992   4 chrome
    238      23    17540      39260       0.05   89428   4 chrome
    413      35   196720     139032      13.22   89640   4 chrome
    238      22    17144      38372       0.06   91668   4 chrome
    257      24    24572      50604       0.20   91984   4 chrome
    263      26   136088     167800       5.44   92396   4 chrome
   1719      92   129468     252564       4.05   89180   4 Cloudflare WARP
    175       9     2164      10240       0.13   17080   4 CompPkgSrv
    135      10     6728       7520       0.05    2656   4 conhost
    129      10     6732      12780       0.02   68888   4 conhost
    269      15     4324      16416       0.11   71760   4 conhost
   3227     157   996868     576816      44.05   89464   4 CorelDRW
    522      37    54368       9056       0.23    2080   4 Cortana
    896      27     2472       6560      20.72     840   0 csrss
    891      37     3816       7784      53.48    6600   4 csrss
    683      24    31848      64432      10.13    6156   4 ctfmon
    168       7     1352       4724       0.02    3540   0 dasHost
    217      18     4236      12036       0.19    7240   0 dllhost
    257      26     6856      15456       0.16   16180   4 dllhost
   1789      71   280096     217152     185.31   10816   4 dwm
    236      13   245264      10036       8.67    5396   0 ElevocControlService
   2932     111   198928     182864      92.28    6372   4 explorer
     50       7     2428       3604       0.27    1104   0 fontdrvhost
     50       9     5068      11156       2.03    4572   4 fontdrvhost
      0       0       60          8                  0   0 Idle
    646      36    25508      19164       0.19   18652   4 IGCC
    442      35    38100      26436       2.22    5596   0 IntelAudioService
    516      36    29624      54332       0.94   13316   4 InterprocessController
    141       9     1372       6252       0.02    5604   0 jhi_service
    326      14    13672      19056      23.45    5676   0 LNBITSSvc
    865      39    63396      61972       1.05    3092   4 LockApp
   1855      31    11276      27336      27.11     772   0 lsass
      0       0     1396     471304      51.42    3220   0 Memory Compression
    398      21    19716      33080       4.39   60572   0 MoUsoCoreWorker
    523      18    12052      21356       9.83    5792   0 MpDefenderCoreService
    262      16     9532      24864       0.19   68688   4 msedge
    199      14     9564      18796       0.30   73512   4 msedge
    375      33   108588      19872       5.41   81264   4 msedge
    213      17    21528      24688       0.13   87772   4 msedge
```

This enumerates currently running user-mode processes

```
                    Get-Process | Sort-Object CPU -Descending | Select-Object -First 10 Name, Id, CPU
>> C:\WINDOWS\system32>

Name          Id         CPU
----          --         ---
System         4 2344.078125
MsMpEng     6080 2141.484375
tailscaled  7416 2030.078125
svchost     2560  2014.78125
sqlservr    4376  1529.09375
warp-svc    5404  908.421875
NisSrv      8304  472.921875
svchost     4248   419.78125
chrome      5584   372.78125
AyuGram    90244  269.046875
```

THIS FILTERS THE HIGEST USE TASK BEING USED BY THE CPU

2. **Delving deeper, it's important to examine how individual applications interact within the larger system framework. Most applications are deliberately confined to operate in what's known as User Mode—a restricted execution environment designed to isolate regular programs from the critical core of the operating system. By running applications in User Mode, the system enforces boundaries, ensuring that these programs cannot directly manipulate hardware resources, interfere with vital components like the kernel, memory manager, or alter system-wide access permissions. This containment not only protects the integrity of the OS but also limits the potential damage that could be caused by faulty or malicious software.**

3. **The rationale behind separating User Mode and Kernel Mode is rooted in both stability and security. The kernel and other core system services operate in Kernel Mode, where they have unrestricted access to all system resources. This privileged access is necessary for the kernel to manage hardware, coordinate processes, and enforce security policies. However, if every application were granted direct access to Kernel Mode, the system would become highly unstable and vulnerable—routine application bugs could crash the entire machine, files could be easily corrupted, and attackers would have a direct avenue to compromise the system's deepest layers.**

4. To enforce system security and stability, the operating system functions as a strict gatekeeper between applications and critical system resources. When a program needs to carry out a privileged action—such as accessing the disk, changing system configurations, or interacting with protected memory—it cannot do so directly. Instead, the request must be submitted through a controlled mechanism called a **system call**. The kernel carefully inspects each request, checks the application's permissions, and evaluates the current system state before deciding whether the operation is allowed. Only requests that meet the defined security policies are executed. This controlled mediation is a core principle of modern operating system design, as it separates user-level processes from kernel-level authority, prevents unauthorized or malicious actions, and maintains overall system reliability.

Set-ExecutionPolicy Restricted

When this command is run without administrative privileges, PowerShell denies the request. This behavior demonstrates how the operating system restricts sensitive configuration changes and requires elevated permissions, reinforcing the role of the kernel as a gatekeeper that controls access to critical system settings.