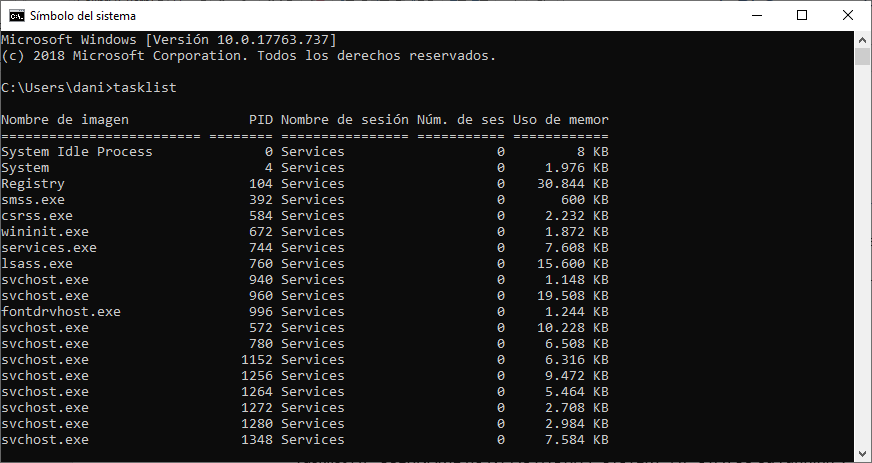
Ejercicios taskList y taskill

Instrucciones : Capture la pantalla de su equipo para mostrar la salida y explicar. Configurar la consola para fondo blanco y letras negras.

1. Desde la línea de comandos (ventana MSDOS) ejecute el comando tasklist. ¿Qué información suministra?



Lista todos los procesos en formato de tabla.

1. Analizar las opciones del comando anterior. ¿Qué información puede obtener de ellas?.

Puede recibir los siguientes parámetros:

/S /U /P : Servidor, usuario y password, respectivamente, para conectarse a un sistema remoto.

/M: lista solo los procesos que utilizan un determinado módulo (.dll).

/FI: permite filtrar los resultados.

/SVC: visualiza los servicios alojados en el proceso.

/APPS: visualiza las aplicaciones de la tienda.

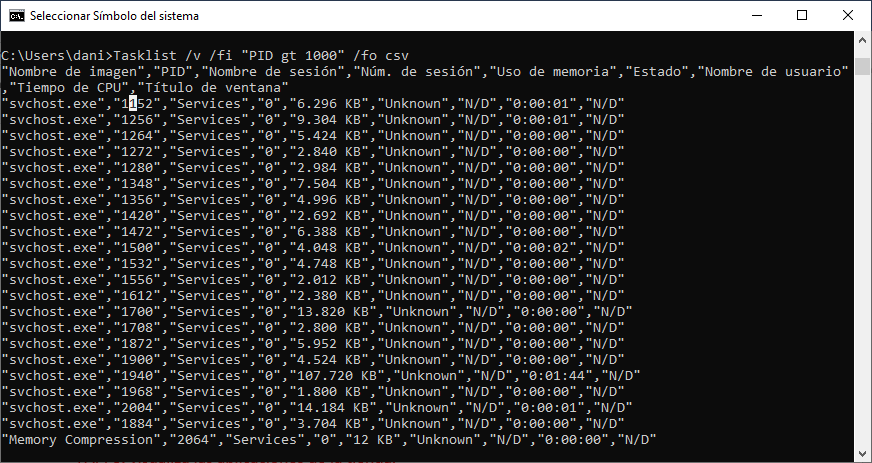
/V: información detallada.

/FO: permite cambiar el formato a tipo TABLA, CSV o lista.

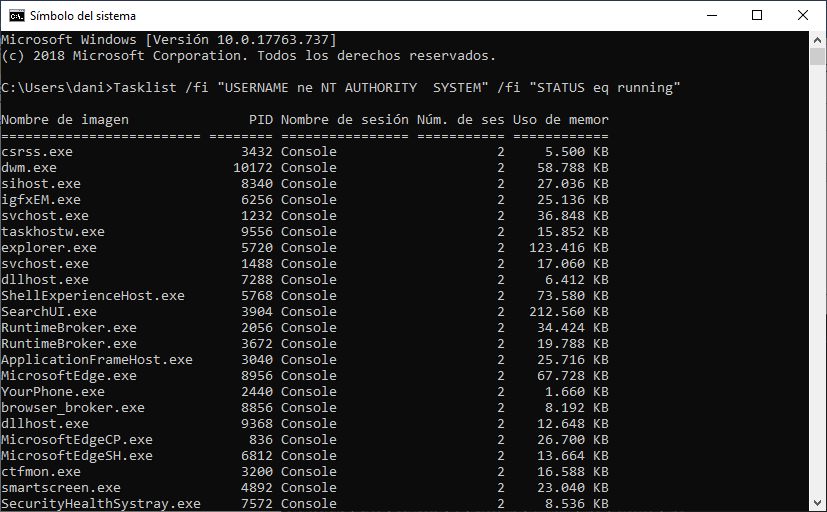
/NH: Elimna la cabecera en el formato tabla y en el CSV.

1. Analizar los siguientes comandos y explique qué hace cada uno de ellos.

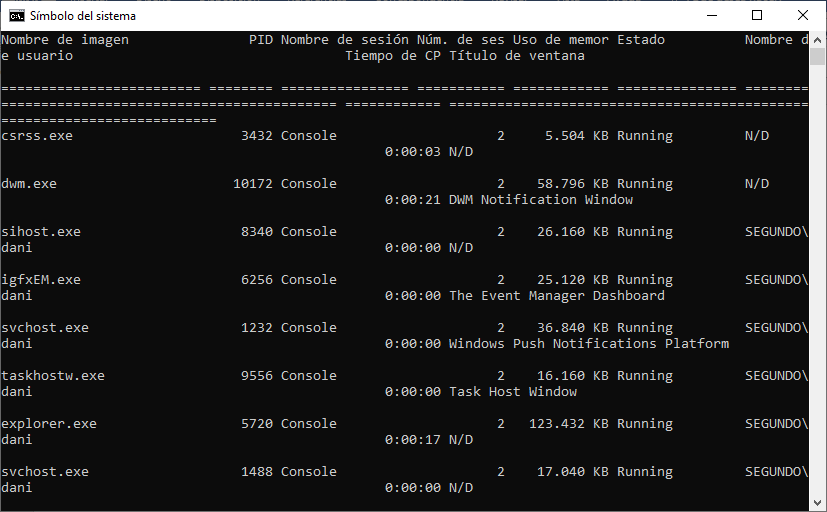
* Tasklist /v /fi “PID gt 1000” /fo csv



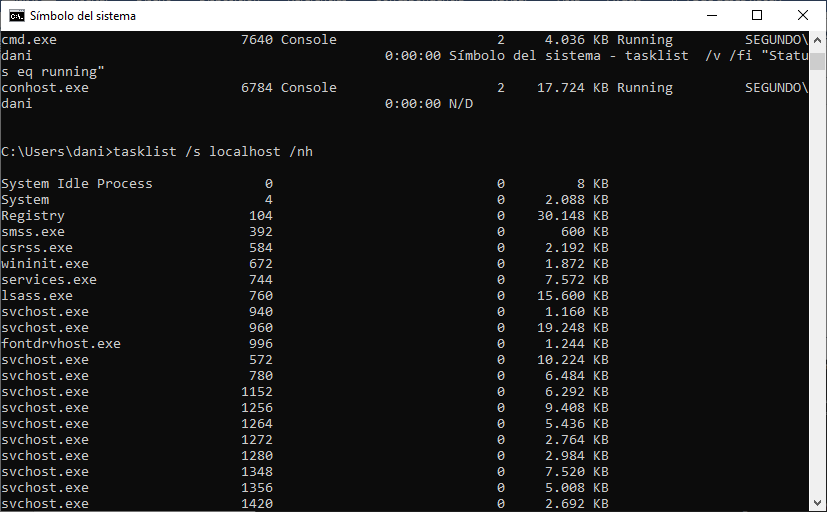
* Tasklist /fi “USERNAME ne NT AUTHORITY SYSTEM” /fi “STATUS eq running”.



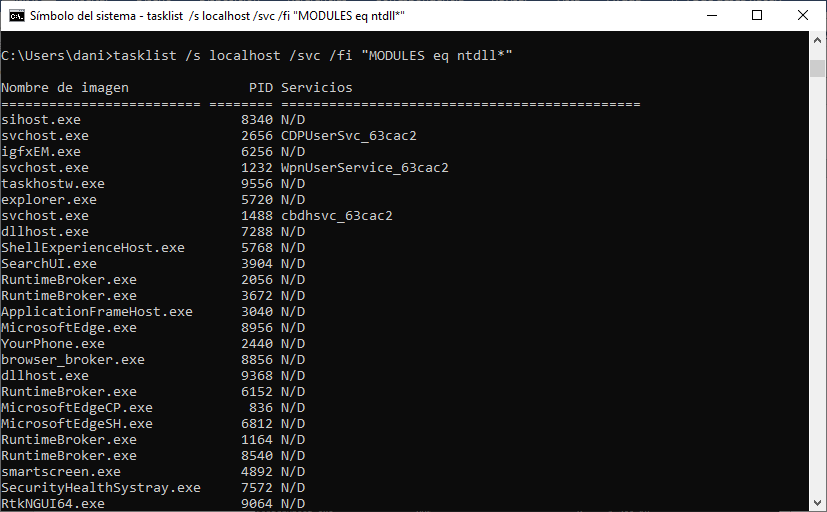
* Tasklist /v /fi “STATUS eq running”



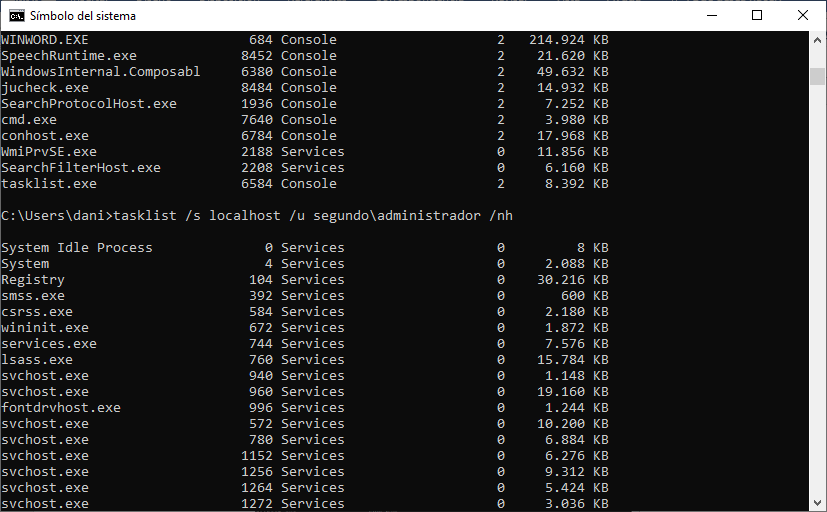
* Tasklist /s srvmain /nh



* Tasklist /s srvmain /svc /fi “MODULES eq ntdll\*”

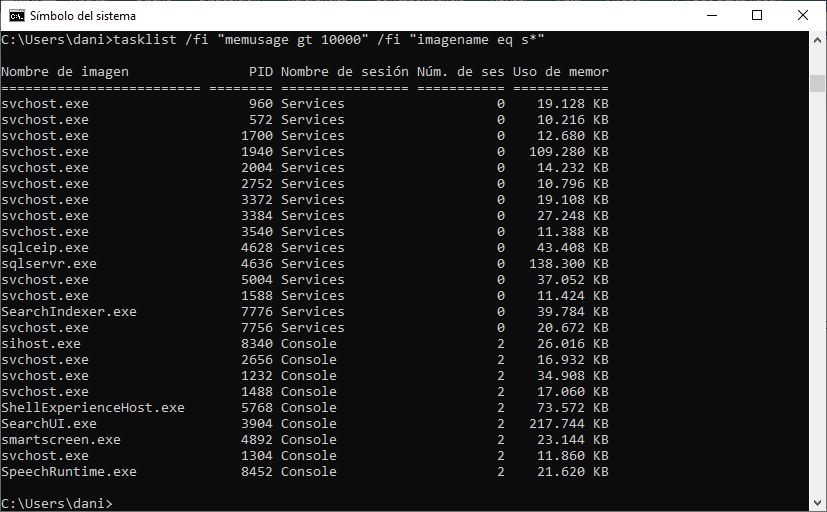


* Tasklist /s srvmain /u maindom\hiropln /p p@ssW23 /nh.



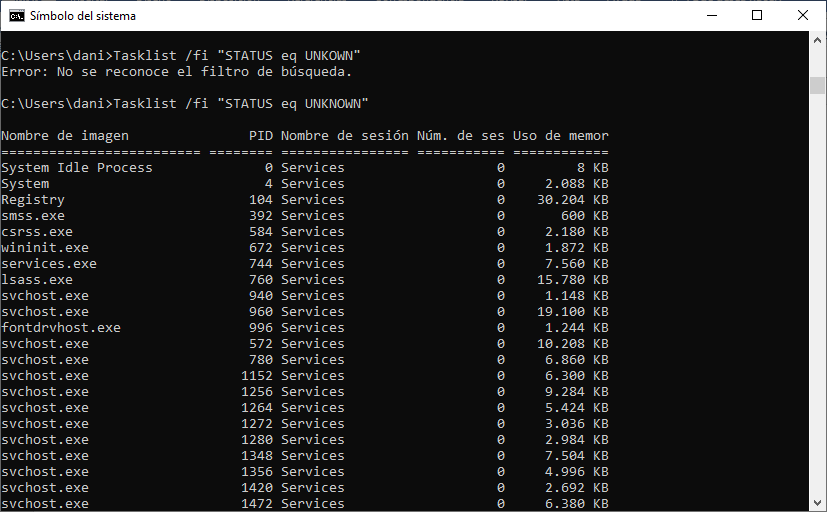
1. Listar todos los procesos cuya imagen empiece por s y que consuman más de 100.000kb de memoria.

Tasklist /fi “MEMUSAGE gt 10000” /fi “IMAGENAME eq S\*”



1. Listar todos los comandos cuyo estado no sea conocido por el sistema.

Tasklist /fi “STATUS eq UNKNOWN”



1. Investigue el comando taskkill.

/S /U /P : Servidor, usuario y password, respectivamente, para conectarse a un sistema remoto.

/IM: Filtra por nombre del ejecutable.

/PID: Filtra por ID de proceso.

/FI: permite filtrar los resultados.

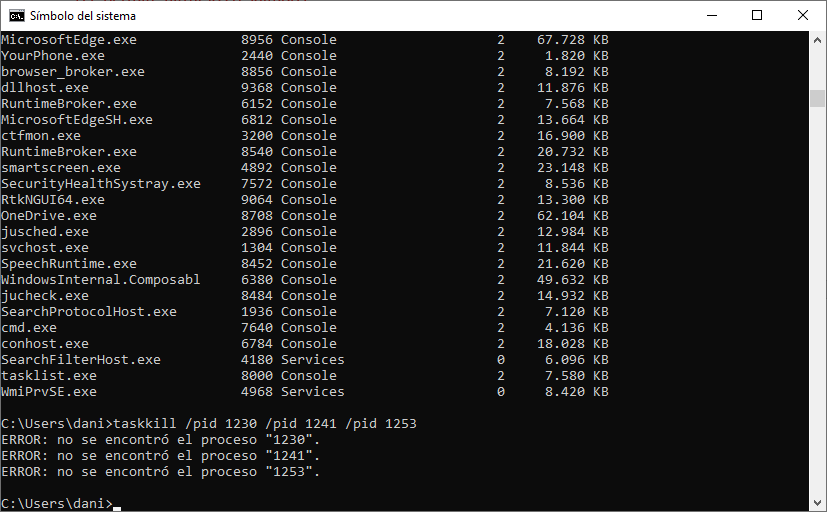
/T: Termina los subproceso.

/F: Fuerza la terminación.

1. Analice los siguientes comandos y explique qué hace cada uno de ellos

* Taskkill /pid 1230 /pid 1241 /pid 1253

Finalizaría los procesos enumerados, como no existe ninguno con esos id, no finaliza ninguno.

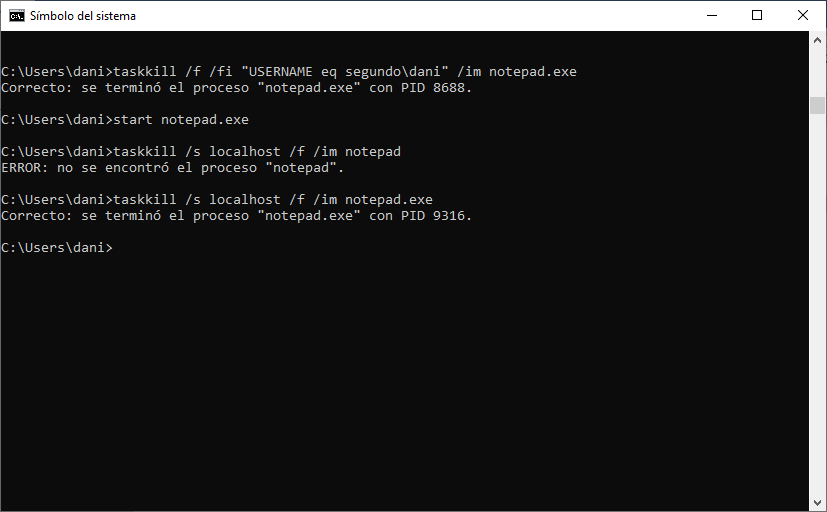


* Taskkill /f /fi“USERNAME eq NT AUTHORITY \SYSTEM” /im notepad.exe

Mata todos los procesos del usuario NT AUTHORITY\SYSTEM cuyo ejecutable sea notepad.exe, pero no hay ninguno.

* Taskkill /s srvmain /f /im notepad.exe

Finaliza el proceso del servidor “srvmain” cuyo nombre de imagen sea notepad.exe



* Taskkill /s srvmain /u maindom\hiropln /p p@ssw23 /fi “IMAGENAME eq note\*”

Finaliza todos los procesos en ejecución del servidor “srvmain”, conectandose como hiropln y cuyo nombre empiece por note..

* Taskkill /s srvmain /u maindom\ hiropln /fi “USERNAME ne NT\*”

Finaliza todos los procesos en ejecución del servidor especificado, logeado con el usuario especificado y cuyo usuario propietario no empiece por NT

* Taskkill /pid 2134 /t /fi “username eq administrador”

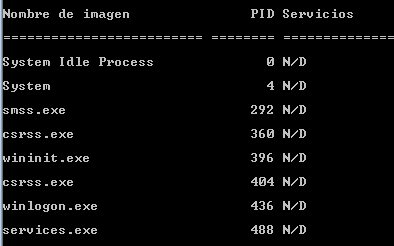
Finaliza el proceso, y todos subprocesos, cuyo id sea 2134 y cuyo usuario propietario sea administrador.

1. Taskkill /f /fi “PID ge 1000”

Fuerza el apagado de todos los procesos que tienen un PID >1000

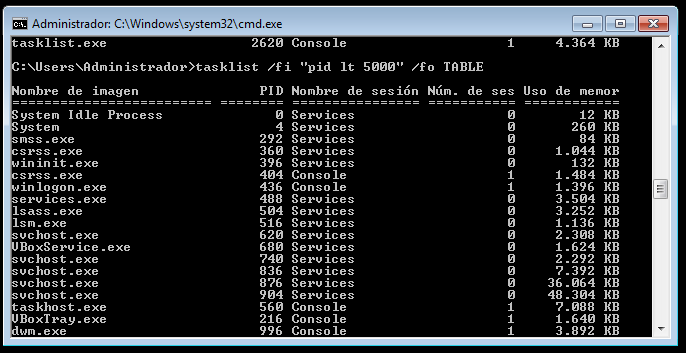
1. Ejecuta tasklist /SVC. ¿Para qué nos sirve?

Sirve para mostrar los servicios asociados a un proceso.



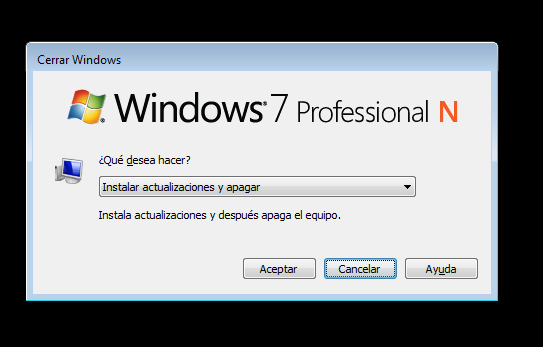
1. Listar los procesos cuyo PID sea mayor que 5000 en formato de tabla.

Tasklist /fi “PID gt 5000”



1. Eliminar todos los procesos cuyo consumo de memoria superen los 100000 kb.

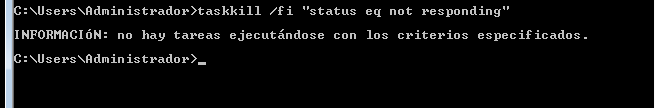
Taskkill /fi “MEMUSAGE gt 100000”



Si cerramos Winlogon.exe nos pide cerrar Windows

1. Eliminar todos los procesos que no estén respondiendo.

Taskkill /fi “STATUS eq NOT RESPONDING”

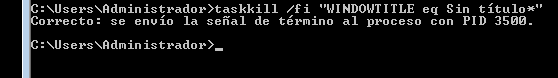


1. Lo mismo pero utilizando /f. ¿cuál es la diferencia?

Taskkill /fi “STATUS eq NOT RESPONDING” /f

La diferencia es que /f fuerza el cierre.

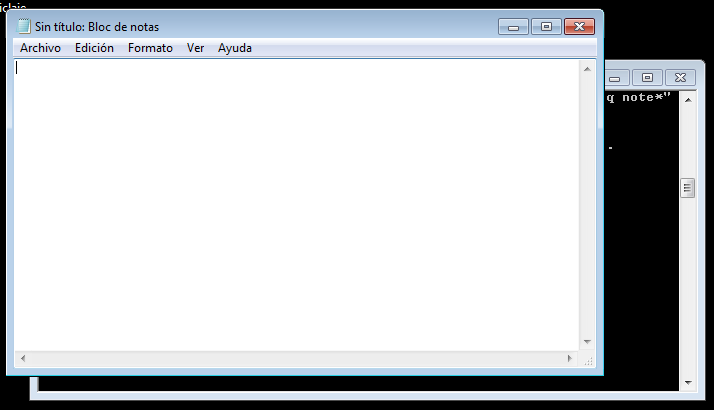
1. Abrir el bloc de notas y cerrarlo mediante taskill utilizando el título de su ventana.



Ejercicios start

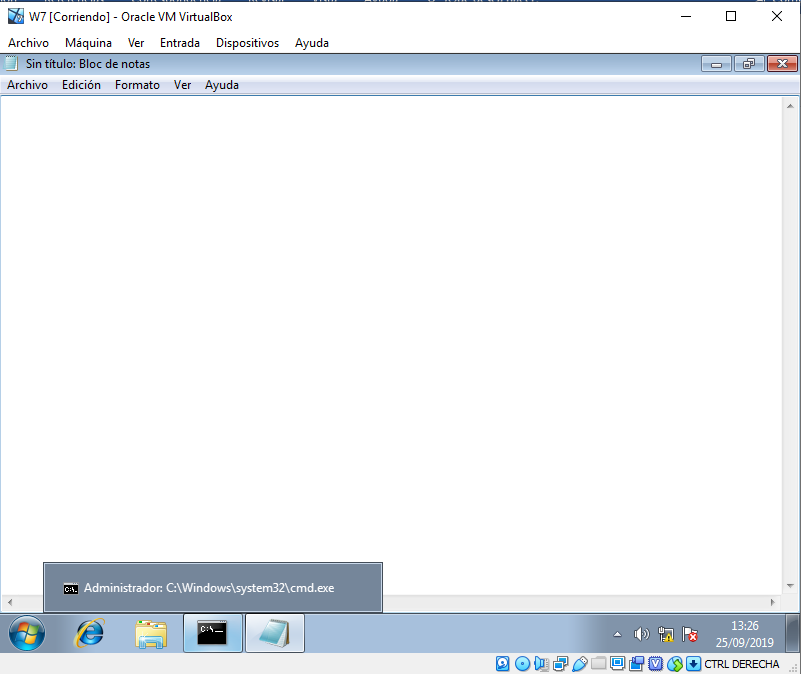
1. Lanzar el bloc de notas.

Start Notepad.exe



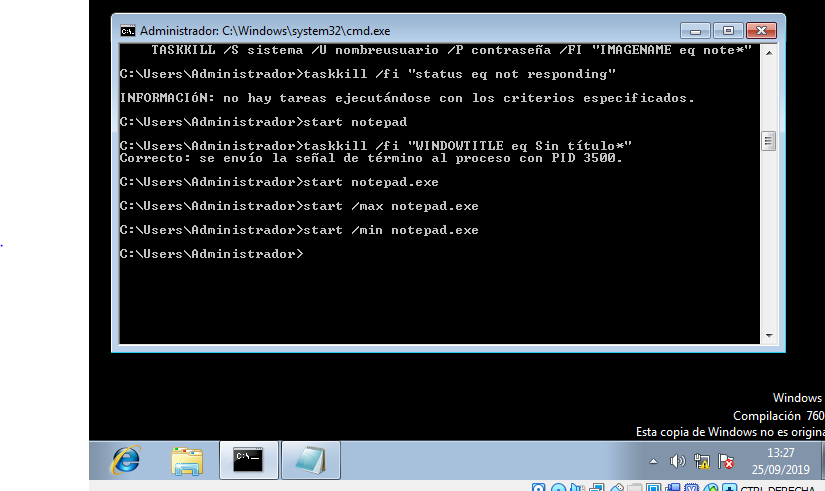
1. Lanzar el bloc de notas maximizado.

start /MAX Notepad.exe



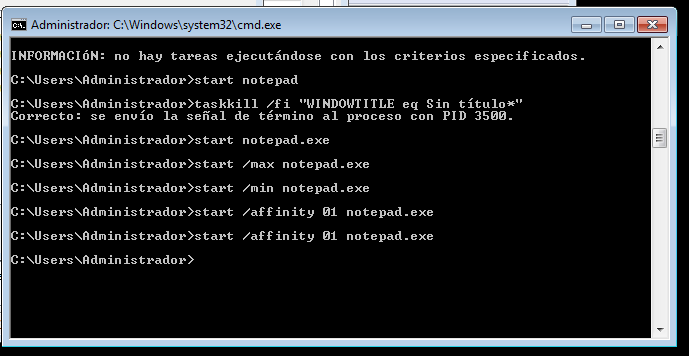
1. Lanzar el bloc de notas minimizado.

start /Min Notepad.exe.



1. Lanzar el bloc de notas para que se ejecute con afinidad para el procesador 1

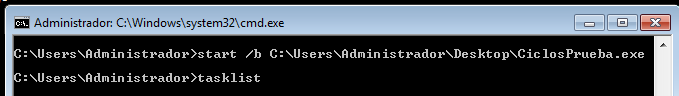
Start /affinity 01 notepad.exe



1. Lanzar ciclosprueba.exe para que se ejecute sin mostrar una nueva pantalla.

Start /b C:\users\Administrador\Desktop\ciclosprueba.exe

1. Comprobar mediante un tasklist si efectivamente se esta ejecutando el proceso.



1. Detenerlo con un taskkill utilizando el pid.

Taskkil /pid 316 /f

1. ¿Se ha podido? En caso contrario utilizar la opción necesaria para hacerlo.

En un principio no, por lo que hemos tenido que usar /f

Ejercicios procesos (ejecutar desde la línea de comandos y repetir desde el administrador de tareas de Windows.)

Realizar las siguientes tareas e ir capturando los pantallazos de las acciones realizadas

1. Localizar *“proceso inactivo del sistema”* y rellena la siguiente información

|  |  |
| --- | --- |
| %CPU | 99 |
| Usuario | System |
| Uso de memoria | 12 |
| Descripción | % tiempo de inactividad del procesador |

¿En qué dirías que consiste?

Es el proceso que mantiene ocupado al sistema mientras no hay ningún otro proceso ejecutándose.

1. Localizar los siguientes procesos y muestra su información.

|  |  |  |  |
| --- | --- | --- | --- |
| INFORMACIÓN | SMSS.EXE | CSRSS.EXE | WINLOGON.EXE |
| %CPU | 0 | 0 | 0 |
| Usuario | System | System | System |
| Uso de memoria | 56 k | 1076/1300 | 1416 |
| Descripción | Administrador de sesión de Windows. | Proceso en tiempo de ejecución c/s | Aplicación de inicio de sesión |

1. Localizar el proceso explorer.exe (no confundir con iexplore.exe) y detenerlo. ¿Qué ha pasado? ¿para qué dirías que sirve?

Se ha cerrado el escritorio. Explorer.exe es el proceso que ejecuta el escritorio de Windows.

1. Localizar el proceso winlogon.exe. Pararlo. ¿Qué ha sucedido? ¿Qué es lo que hay que hacer antes de realizar cualquier tarea administrativa?

Se ha cerrado la sesión del usuario actual.

Antes de cualquier tarea administrativa hay que guardar cambios y hacer copia de seguridad o punto de restauración.

1. Localizar el proceso smss.exe y detenerlo. ¿Qué ha sucedido? ¿Qué dirías que es este proceso?

Es el administrador de sesión, sale el cuadro de apagar equipo.

1. Lanzar el proceso cmd.exe. Anota el id del proceso: 1508
2. Vuelve a ejecutarlo, sin eliminar el anterior. ¿Cuántos procesos hay con el mismo nombre de imagen? ¿Cuál es la diferencia entre programa y proceso?

Hay dos el 1508 y el 8796

1. Realizar lo mismo con la opción /b. ¿Qué ha pasado?

Lanza el proceso cmd en la misma ventana de la interfaz de usuario.

1. Lanzar CiclosPrueba y ver la información de dicho proceso.

Pid 3964, uso de memoria 11800

1. Abrir la pestaña rendimiento. Cambiar la afinidad de CiclosPrueba. ¿Qué ha pasado?

Ahora la CPU elegida tiene el 100% de consumo y el resto está desocupada.

1. Ejecutar varias instancias del mismo programa y cambiar la afinidad de los mismos para que cada uno tenga afinidad por un procesador diferente. Comprobar el efecto en la carga de las distintas CPU.

Todos los procesadores se cargan al 100%

1. Volver a establecer la afinidad en todos los procesadores, para los procesos creados anteriormente.

El sistema balancearía las cargas