

PR0302: Introducción a Powershell (II)

Nombre/s: Alejandro Prieto Pellitero

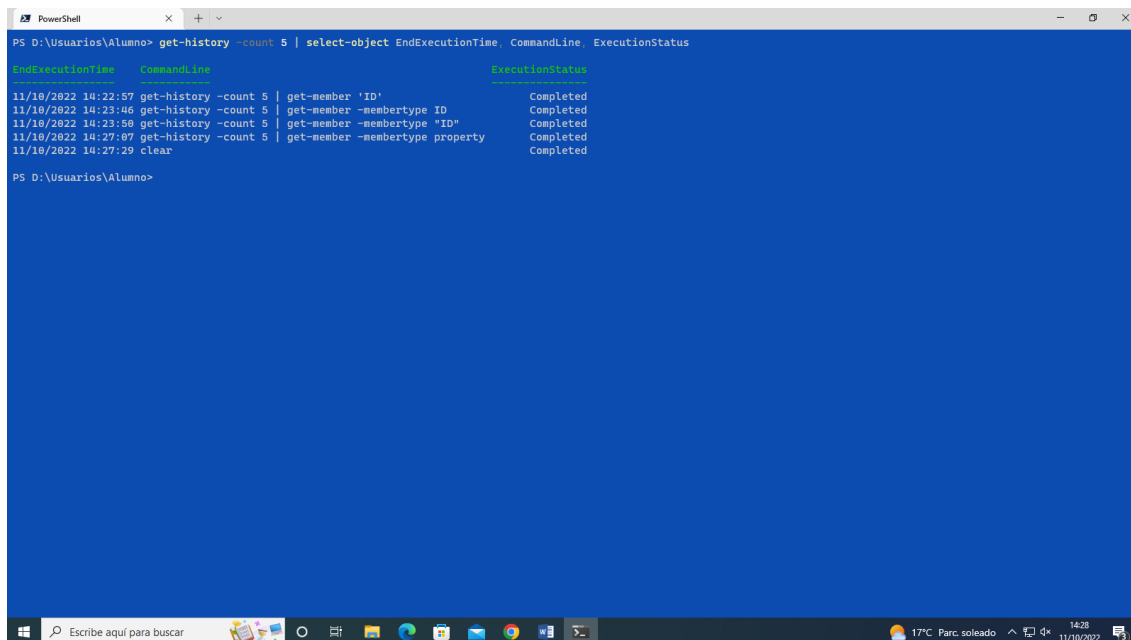
Tienes que contestar las preguntas en este mismo fichero después de cada pregunta. No te olvides de poner tu nombre en el recuadro superior.

Quando hayas acabado todas las prácticas renombas el fichero para que se llame **{Apellido1} {Apellido2}, {Nombre} - PR0201**. En el nombre y apellidos la primera mayúscula y el resto en minúsculas. El fichero tiene que estar en formato PDF. Cualquier fichero que no siga esta nomenclatura o no esté en PDF no será corregido. El fichero final lo tienes que subir a la plataforma.

Ejercicio 1: Powershell

Realiza las siguientes tareas que se te piden utilizando Powershell. Para contestar lo mejor es que hagas una captura de pantalla donde se vea el comando que has introducido y las primeras líneas de la salida de este.

1.- Visualiza las últimas cinco entradas del historial, mostrando para cada una el comando, la hora en que finalizó su ejecución y el estado de ejecución.



```
PS D:\Usuarios\Alumno> get-history -count 5 | select-object EndExecutionTime, CommandLine, ExecutionStatus

EndExecutionTime    CommandLine          ExecutionStatus
-----
11/10/2022 14:22:57  get-history -count 5 | get-member 'ID'           Completed
11/10/2022 14:23:46  get-history -count 5 | get-member -membertype ID  Completed
11/10/2022 14:23:50  get-history -count 5 | get-member -membertype "ID" Completed
11/10/2022 14:27:07  get-history -count 5 | get-member -membertype property Completed
11/10/2022 14:27:29  clear               Completed

PS D:\Usuarios\Alumno>
```

2.- Ejecuta el comando **Get-Command** (que muestra todos los comandos disponibles en Powershell) e interrúmpelo antes de que finalice su ejecución pulsando las teclas Ctrl-C. A continuación, ejecútalo dejando que finalice correctamente.

```

PowerShell
Function Get-ScheduledTask 1.0.0.0 ScheduledTasks
Function Get-ScheduledTaskInfo 1.0.0.0 ScheduledTasks
Function Get-SmbBandwidthLimit 2.0.0.0 SmbShare
Function Get-SmbClientConfiguration 2.0.0.0 SmbShare
Function Get-SmbClientNetworkInterface 2.0.0.0 SmbShare
Function Get-SmbConnection 2.0.0.0 SmbShare
Function Get-SmbDelegation 2.0.0.0 SmbShare
Function Get-SmbGlobalMapping 2.0.0.0 SmbShare
Function Get-SmbMapping 2.0.0.0 SmbShare
Function Get-SmbMultichannelConnection 2.0.0.0 SmbShare
Function Get-SmbMultichannelConstraint 2.0.0.0 SmbShare
Function Get-SmbOpenFile 2.0.0.0 SmbShare
Function Get-SmbServerCertificateMapping 2.0.0.0 SmbShare
Function Get-SmbServerConfiguration 2.0.0.0 SmbShare
Function Get-SmbServerNetworkInterface 2.0.0.0 SmbShare
Function Get-SmbSession 2.0.0.0 SmbShare
Function Get-SmbShare 2.0.0.0 SmbShare
Function Get-SmbShareAccess 2.0.0.0 SmbShare
Function Get-SmbWitnessClient 2.0.0.0 SmbWitness
PS D:\Usuarios\Alumno> get-command

CommandName Name Version Source
-----
Alias Add-AppPackage 2.0.1.0 Appx
Alias Add-AppPackageVolume 2.0.1.0 Appx
Alias Add-AppProvisionedPackage 3.0 Dism
Alias Add-ProvisionedAppPackage 3.0 Dism
Alias Add-ProvisionedAppPackage 3.0 Dism
Alias Add-ProvisioningPackage 3.0 Provisioning
Alias Add-TrustedProvisioningCertificate 3.0 Provisioning
Alias Apply-WindowsUnattend 3.0 Dism
Alias Disable-PhysicalDiskIndication 2.0.0.0 Storage
Alias Disable-StorageDiagnosticLog 2.0.0.0 Storage
Alias Dismount-AppPackageVolume 2.0.1.0 Appx
Alias Enable-PhysicalDiskIndication 2.0.0.0 Storage
Alias Enable-StorageDiagnosticLog 2.0.0.0 Storage
Alias Export-VMCheckpoint 2.0.0.0 Hyper-V
Alias Flush-Volume 2.0.0.0 Storage
Alias Get-AppPackage 2.0.1.0 Appx
Alias Get-AppPackageDefaultVolume 2.0.1.0 Appx
Alias Get-AppPackageLastError 2.0.1.0 Appx
Alias Get-AppPackageLog 2.0.1.0 Appx

```

3.- Vuelve a ejecutar el comando del punto 1 y comprueba las diferentes salidas de finalización de estado de ejecución.

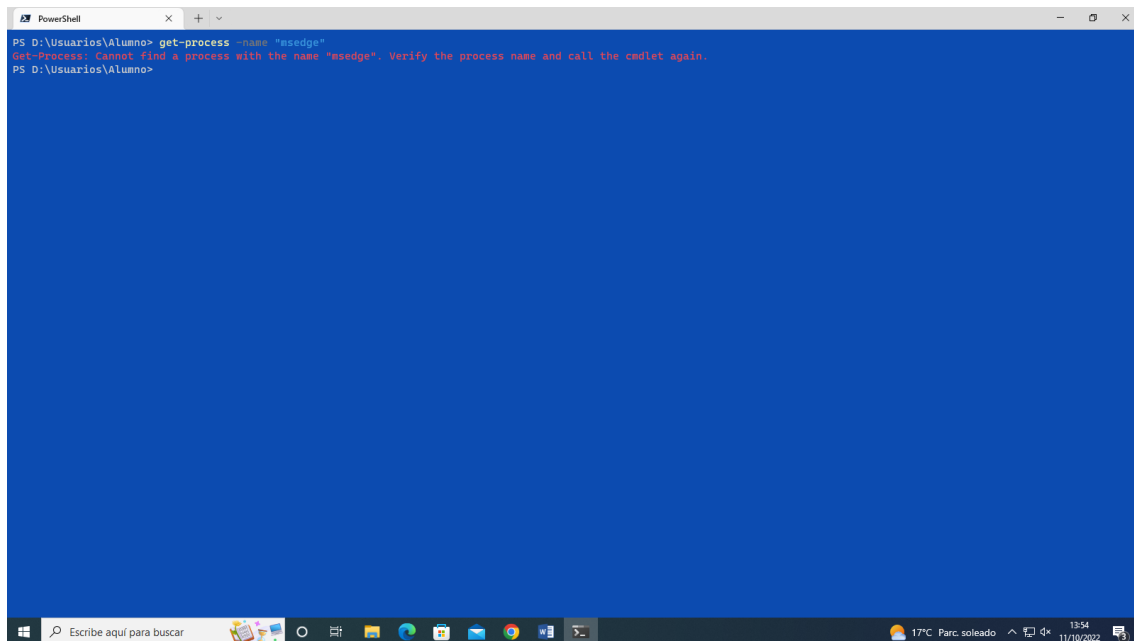
```

PowerShell
PS D:\Usuarios\Alumno> get-history -count 5 | select-object EndExecutionTime, CommandLine, ExecutionStatus

EndExecutionTime CommandLine ExecutionStatus
-----
11/10/2022 14:22:57 get-history -count 5 | get-member 'ID' Completed
11/10/2022 14:23:46 get-history -count 5 | get-member -membertype ID Completed
11/10/2022 14:23:56 get-history -count 5 | get-member -membertype "ID" Completed
11/10/2022 14:27:07 get-history -count 5 | get-member -membertype property Completed
11/10/2022 14:27:29 clear Completed
PS D:\Usuarios\Alumno>

```

4.- Muestra todos los procesos con el nombre *msedge* mostrando para cada uno el identificador, el consumo de CPU y los hilos (*threads*)

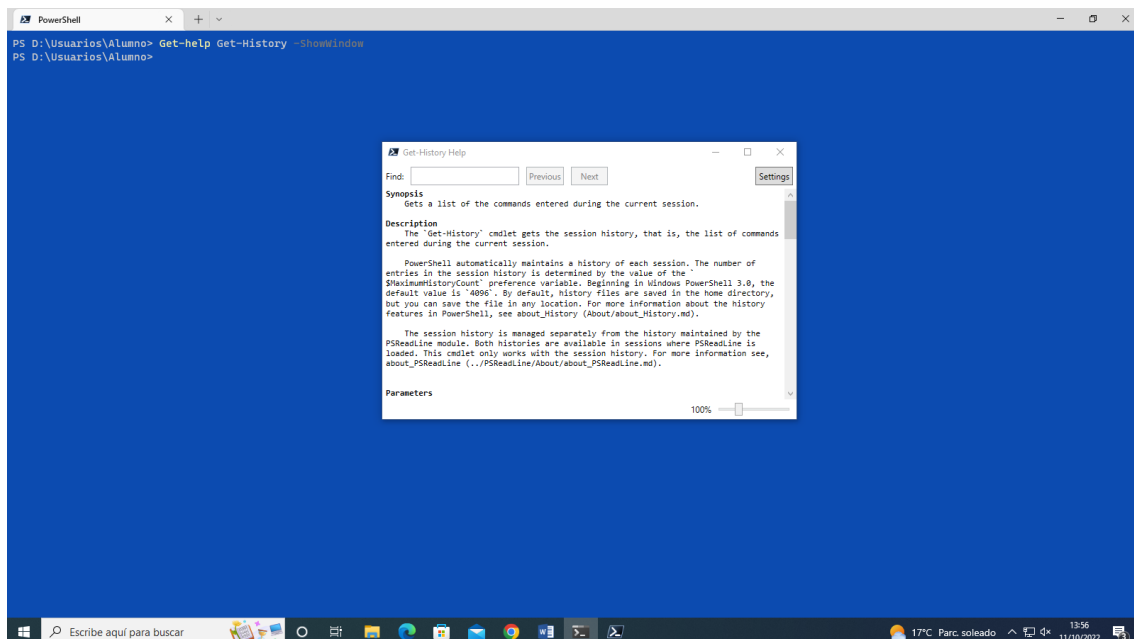


A screenshot of a Windows PowerShell window. The title bar says "PowerShell". The command prompt shows the user is in the directory "D:\Usuarios\Alumno". The user has entered the command `get-process -name "esedge"`. The output is an error message: `Get-Process: Cannot find a process with the name "esedge". Verify the process name and call the cmdlet again.` The prompt is now `PS D:\Usuarios\Alumno>`. The taskbar at the bottom shows the search bar, task view, and several application icons. The system tray shows the temperature as 17°C, weather as "Parc. soleado", and the time as 13:54 on 11/10/2022.

5.- Averigua para qué sirve el parámetro **-Delimiter** del comando **Export-CSV**

Especifica con qué separar los valores de las propiedades

6.- Muestra en una ventana la ayuda del comando **Get-History**



A screenshot of a Windows PowerShell window. The title bar says "PowerShell". The command prompt shows the user is in the directory "D:\Usuarios\Alumno". The user has entered the command `Get-help Get-History -ShowWindow`. The prompt is now `PS D:\Usuarios\Alumno>`. A help window titled "Get-History Help" is open in the foreground. It contains the following information:
Synopsis
Gets a list of the commands entered during the current session.
Description
The "Get-History" cmdlet gets the session history, that is, the list of commands entered during the current session.
PowerShell automatically maintains a history of each session. The number of entries in the session history is determined by the value of the `$MaximalHistoryCount` preference variable. Beginning in Windows PowerShell 3.0, the default value is "4096". By default, history files are saved in the home directory, but you can save the file in any location. For more information about the history features in PowerShell, see `about_History` (`about/about_History.md`).
The session history is managed separately from the history maintained by the `PSReadLine` module. Both histories are available in sessions where `PSReadLine` is loaded. This cmdlet only works with the session history. For more information see, `about_PSReadLine` (`../PSReadLine/About/about_PSReadLine.md`).
Parameters
The window has a search bar, "Previous" and "Next" buttons, and a "Settings" button. A scrollbar is visible on the right side of the text area. The taskbar at the bottom shows the search bar, task view, and several application icons. The system tray shows the temperature as 17°C, weather as "Parc. soleado", and the time as 13:56 on 11/10/2022.

7.- Muestra un listado con todos los comandos que tengan el verbo *Update*.

```
PowerShell
Get-Help
Get-Member
Get-PSDrive
Import-PSSession
about_Command_Precedence

PS D:\Usuarios\Alumno> Get-Command -verb "update"

CommandType Name Version Source
-----
Function Update-AutoLoggerConfig 1.0.0.0 EventTracingManagement
Function Update-Disk 2.0.0.0 Storage
Function Update-DscConfiguration 1.1 PSDesiredStateConfiguration
Function Update-EtwTraceSession 1.0.0.0 EventTracingManagement
Function Update-HostStorageCache 2.0.0.0 Storage
Function Update-IscsiTarget 1.0.0.0 iSCSI
Function Update-IscsiTargetPortal 1.0.0.0 iSCSI
Function Update-Module 2.2.5 PowerShellGet
Function Update-ModuleManifest 1.0.0.1 PowerShellGet
Function Update-ModuleManifest 2.2.5 PowerShellGet
Function Update-ModuleManifest 1.0.0.1 PowerShellGet
Function Update-MpSignature 1.0 ConfigDefender
Function Update-MpSignature 1.0 Defender
Function Update-NetFirewallDynamicKeywordAddress 2.0.0.0 NetSecurity
Function Update-NetIPsecRule 2.0.0.0 NetSecurity
Function Update-Script 2.2.5 PowerShellGet
Function Update-Script 1.0.0.1 PowerShellGet
Function Update-ScriptFileInfo 2.2.5 PowerShellGet
Function Update-ScriptFileInfo 1.0.0.1 PowerShellGet
Function Update-SmbMultichannelConnection 2.0.0.0 SmbShare
Function Update-StorageFirmware 2.0.0.0 Storage
Function Update-StoragePool 2.0.0.0 Storage
Function Update-StorageProviderCache 2.0.0.0 Storage
Cmdlet Update-FormatData 7.0.0.0 Microsoft.PowerShell.Utility
Cmdlet Update-Help 7.2.6.500 Microsoft.PowerShell.Core
Cmdlet Update-List 7.0.0.0 Microsoft.PowerShell.Utility
Cmdlet Update-TypeData 7.0.0.0 Microsoft.PowerShell.Utility
Cmdlet Update-VMVersion 2.0.0.0 Hyper-V
Cmdlet Update-WIMBootEntry 3.0 Dism

PS D:\Usuarios\Alumno> |
```

8.- Ejecuta la herramienta *Recortes* y localízala usando el comando **Get-Process** teniendo en cuenta que el proceso se llama *SnippingTool.exe*

```
PowerShell
PS D:\Usuarios\Alumno> get-process -name "SnippingTool"

Name PID PM PIDL PPID PID PPID Name
----
18 5,41 21,66 0,19 12236 1 SnippingTool

PS D:\Usuarios\Alumno>
```

9.- Averigua qué propiedades tienen los procesos devueltos con el comando **Get-Process**.

```
PowerShell
PS D:\Usuarios\Alumno> gps SnippingTool | get-member

TypeName: System.Diagnostics.Process

Name MemberType Definition
-----
Handles AliasProperty Handles = HandleCount
Name AliasProperty Name = ProcessName
NPM AliasProperty NPM = NonpagedSystemMemorySize64
PM AliasProperty PM = PagedMemorySize64
SI AliasProperty SI = SessionId
VM AliasProperty VM = VirtualMemorySize64
WS AliasProperty WS = WorkingSet64
Parent CodeProperty System.Object Parent{get:GetParentProcess;}
Disposed Event System.EventHandler Disposed(System.Object, System.EventArgs)
ErrorDataReceived Event System.Diagnostics.DataReceivedEventHandler ErrorDataReceived(System.Object, System.Diagnostics.DataReceivedEventArgs)
Exited Event System.EventHandler Exited(System.Object, System.EventArgs)
OutputDataReceived Event System.Diagnostics.DataReceivedEventHandler OutputDataReceived(System.Object, System.Diagnostics.DataReceivedEventArgs)
BeginErrorReadLine Method void BeginErrorReadLine()
BeginOutputReadLine Method void BeginOutputReadLine()
CancelErrorRead Method void CancelErrorRead()
CancelOutputRead Method void CancelOutputRead()
Close Method void Close()
CloseMainWindow Method bool CloseMainWindow()
Dispose Method void Dispose(), void IDisposable.Dispose()
Equals Method bool Equals(System.Object obj)
GetHashCode Method int GetHashCode()
GetLifetimeService Method System.Object GetLifetimeService()
GetType Method type GetType()
InitializeLifetimeService Method System.Object InitializeLifetimeService()
Kill Method void Kill(), void Kill(bool entireProcessTree)
Refresh Method void Refresh()
Start Method bool Start()
ToString Method string ToString()
WaitForExit Method void WaitForExit(), bool WaitForExit(int milliseconds)
WaitForExitAsync Method System.Threading.Tasks.Task WaitForExitAsync(System.Threading.CancellationToken cancellationToken)
WaitForInputIdle Method bool WaitForInputIdle(), bool WaitForInputIdle(int milliseconds)
__Vtable__ NoteProperty string __Vtable__=Process
BasePriority Property int BasePriority {get;}
Container Property System.ComponentModel.IContainer Container {get;}
EnableRaisingEvents Property bool EnableRaisingEvents {get;set;}
ExitCode Property int ExitCode {get;}
```

10.- Busca en la ayuda para qué sirve el parámetro **-MemberType** del comando **Get-Member**.

Especifica el tipo de miembro

11.- Desde la línea de comandos, finaliza la ejecución de la herramienta *recortes*.

```
PowerShell
PS D:\Usuarios\Alumno> gps SnippingTool | stop-process
PS D:\Usuarios\Alumno>
```

12.- Muestra todos los procesos que tienen el nombre *svchost*.

```

PS D:\Usuarios\Alumno> ps -svchost

Name      PID      PName      CPU      Private      ID      ProcessName
-----
23      10,93      26,85      0,00      568      0      svchost
24      8,38      32,94      1,00      648      1      svchost
20      7,77      14,87      0,00      1632     0      svchost
13      2,71      7,90      0,00      1888     0      svchost
84      84,33      35,69      0,00      1888     0      svchost
16      1,83      6,82      0,00      1176     0      svchost
8        1,11      4,89      0,00      1268     0      svchost
18      6,47      14,66      0,00      1332     0      svchost
12      2,08      8,94      0,00      1364     0      svchost
13      3,18      12,72      0,00      1372     0      svchost
10      1,97      7,92      0,00      1460     0      svchost
10      2,60      9,28      0,00      1468     0      svchost
14      5,96      8,84      0,00      1552     0      svchost
19      11,78      18,71      0,00      1612     0      svchost
7        1,44      5,54      0,00      1632     0      svchost
7        1,23      4,72      0,00      1636     0      svchost
15      16,81      15,14      0,00      1648     0      svchost
9        1,98      11,20      0,00      1656     0      svchost
11      1,77      7,42      0,00      1664     0      svchost
8        1,36      6,27      0,00      1888     0      svchost
26      5,18      6,65      0,00      1972     0      svchost
12      2,21      10,18      0,00      2032     0      svchost
10      2,31      7,80      0,00      2060     0      svchost
9        1,84      7,05      0,00      2120     0      svchost
15      4,38      11,15      0,00      2152     0      svchost
11      2,76      8,48      0,00      2256     0      svchost
15      98,89      99,90      0,00      2336     0      svchost
11      1,75      7,05      0,00      2344     0      svchost
7        1,28      5,42      0,00      2364     0      svchost
11      2,46      9,13      0,00      2444     0      svchost
9        1,83      7,09      0,00      2456     0      svchost
13      2,98      11,82      0,00      2672     0      svchost
32      15,54      17,65      0,00      2692     0      svchost
11      9,82      17,51      0,00      2756     0      svchost
14      3,53      7,79      0,00      2792     0      svchost
11      1,59      5,77      0,00      2800     0      svchost
14      2,23      8,42      0,00      2808     0      svchost
13      2,15      10,71      0,00      2912     0      svchost

```

13.- Muestra por pantalla el número de instancias del proceso *svchost*.

14.- Muestra por pantalla todos los procesos con el nombre *svchost* mostrando para cada uno: nombre, identificador, hora de inicio, tiempo total de procesador y clase de prioridad. Se deben mostrar de forma tabular.

```

PS D:\Usuarios\Alumno> get-history -count 5 | select-object EndExecutionTime, CommandLine, ExecutionStatus

EndExecutionTime      CommandLine                                     ExecutionStatus
-----
11/10/2022 14:22:57    get-history -count 5 | get-member 'ID'          Completed
11/10/2022 14:23:46    get-history -count 5 | get-member -membertype ID Completed
11/10/2022 14:23:50    get-history -count 5 | get-member -membertype "ID" Completed
11/10/2022 14:27:07    get-history -count 5 | get-member -membertype property Completed
11/10/2022 14:27:29    clear                                             Completed

```

15.- Repite la búsqueda anterior, pero ordenando por el campo *tiempo total de procesador* en sentido descendente.

```
PowerShell
PS D:\Usuarios\Alumno> get-process -name "svchost" | select-object TotalProcessorTime, Id, Name, StartTime | Sort-Object TotalProcessorTime
```

TotalProcessorTime	Id	Name	StartTime
364	svchost		
3944	svchost		
3800	svchost		
3748	svchost		
3684	svchost		
3616	svchost		
3576	svchost		
4092	svchost		
3436	svchost		
3364	svchost		
3348	svchost		
3180	svchost		
3140	svchost		
3060	svchost		
2968	svchost		
3376	svchost		
9884	svchost		
4368	svchost		
4512	svchost		
9360	svchost		
9316	svchost		
9236	svchost		
8584	svchost		
7620	svchost		
7608	svchost		
4424	svchost		
6828	svchost		
6376	svchost		
6260	svchost		
6212	svchost		
5360	svchost		
5024	svchost		
4652	svchost		
6740	svchost		
2988	svchost		
2916	svchost		
2884	svchost		
1552	svchost		

16.- Muestra los usuarios que hay en el sistema agrupándolos por la propiedad *Enabled*.

```
PowerShell
PS D:\Usuarios\Alumno> Get-LocalUser | Group-Object enabled
```

Count	Name	Enabled
3	False	{DefaultAccount, Invitado, WDAGUtilityAccount}
2	True	{Administrador, Alumno}

```
PS D:\Usuarios\Alumno>
```

17.- Muestra los usuarios que hay en el sistema con la cuenta habilitada (propiedad *Enabled* puesta a *True*). Utiliza el filtrado con el comando **Where-Object**

```
PowerShell
PS D:\Usuarios\Alumno> Get-LocalUser | Where-Object enabled

Name          Enabled Description
-----          -----
Administrador True      Cuenta integrada para la administración del equipo o dominio
Alumno         True
```

18.- Muestra un listado de todos los usuarios del sistema con el nombre y la fecha de la última vez que iniciaron sesión (tienes que buscar la propiedad que indique último inicio de sesión o *last logon*)

```
PowerShell
PS D:\Usuarios\Alumno> Get-LocalUser | Select-object name, lastlogon

Name          LastLogon
-----          -----
Administrador  07/09/2022 8:44:05
Alumno         13/10/2022 8:44:38
DefaultAccount
Invitado
WDAGUtilityAccount
```