Ciclo: Administración de Sistemas Informáticos en Red

Módulo: IMPLANTACIÓN DE SISTEMAS OPERATIVOS

Grupo: 1º ASIR

PR0302: Introducción a Powershell (II)

Nombre/s: Agustín Ruppel Romero

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

Cuando hayas acabado todas las prácticas renombras el fichero para que se llame **{Apellido1} {Apellido2}, {Nombre} – PR0302**. 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.- El comando **Get-Date** muestra la fecha y hora actual. Muestra por pantalla únicamente el año en que estamos.

```
PS D:\Usuarios\Alumno> Get-Date | Select-Object year

Year
----
2022


PS D:\Usuarios\Alumno>
```

2.- Uno de los requisitos de Windows 11 es que es procesador tenga TPM habilitado. Powershell dispone del comando **Get-TPM** que nos muestra información sobre este módulo. Muestra por pantalla, en formato tabla, las propiedades **TpmPresent**, **TpmReady**, **TpmEnabled** y **TpmActivated**.

```
PS C:\Windows\system32> Get-TPM | Format-Table | Select-Object TpmPresent, TpmReady, TpmEnabled, TpmActivated.

TpmPresent TpmReady TpmEnabled TpmActivated.
---------- -------- ---------- -------------
```

En los siguientes ejercicios trabajaremos con los ficheros devueltos por el comando **Get-ChildItem C:\Windows\System32**.

3.- Muestra por pantalla el número de ficheros y directorios que hay en ese directorio.

```
PS C:\Windows\system32> Get-ChildItem  C:\Windows\System32 | Measure-Object


Count    : 4631
Average  :
Sum      :
Maximum  :
Minimum  :
Property :
```

4.- Los objetos devueltos por el comando anterior tienen una propiedad denominada **Extension**, que indica la extensión del archivo. Calcula el número de ficheros en el directorio que tienen la extensión **.dll**.

```
PS C:\Windows\system32> Get-ChildItem *.dll | Measure


Count    : 3440
Average  :
Sum      :
Maximum  :
Minimum  :
Property :



PS C:\Windows\system32>
```

5.- Muestra los ficheros del directorio con extensión **.exe** que tengan un tamaño superior a 50000 bytes.

```
PS C:\Windows\system32> Get-ChildItem C:/Windows\System32 | Where-Object Length -gt 50000


    Directorio: C:\Windows\System32


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        07/12/2019     10:09         195443 @windows-hello-V4.1.gif
-a----        13/10/2022      9:11         488960 aadauthhelper.dll
-a----        13/10/2022      9:11        1107968 aadcloudap.dll
-a----        06/09/2022     13:07          98816 aadjcsp.dll
-a----        13/10/2022      9:11        1419776 aadtb.dll
-a----        13/10/2022      9:11         171856 aadWamExtension.dll
-a----        06/09/2022     13:06         461824 AarSvc.dll
-a----        06/09/2022     13:08         442224 AboutSettingsHandlers.dll
-a----        21/09/2022     11:05         418816 AboveLockAppHost.dll
-a----        09/04/2021     15:57         281088 accessibilitycpl.dll
-a----        09/04/2021     15:58         274432 accountaccessor.dll
-a----        09/04/2021     15:58         435712 AccountsRt.dll
-a----        13/10/2022      9:12         377856 AcGenral.dll
-a----        06/09/2022     13:11         326144 AcLayers.dll
-a----        07/12/2019     10:09         587264 aclui.dll
-a----        06/09/2022     13:07         479560 acmigration.dll
-a----        06/09/2022     13:06         220160 ACPBackgroundManagerPolicy.dll
-a----        09/04/2021     15:57          88576 acppage.dll
-a----        09/04/2021     15:58          81408 AcSpecfc.dll
-a----        09/04/2021     15:57         322048 ActionCenter.dll
-a----        09/04/2021     15:57         166400 ActionCenterCPL.dll
-a----        07/12/2019     10:09         189752 ActionQueue.dll
-a----        09/04/2021     15:56          56320 ActivationClient.dll
-a----        20/09/2022     12:56         802816 ActivationManager.dll
-a----        06/09/2022     13:11         371448 ActivationVdev.dll
```

6.- Muestra los ficheros de este directorio que tengan extensión **.dll**, ordenados por fecha de creación y mostrando únicamente las propiedades de fecha de creación (*CreationTime*), último acceso (*LastAccessTime*) y nombre (*Name*).

```
PS C:\Windows\system32> Get-ChildItem C:/Windows\System32 | Where-Object Extension -eq .dll | Select-Object CreationTime, LastAccessTime, Name

CreationTime        LastAccessTime      Name
------------        --------------      ----
07/12/2019 10:09:55 27/09/2022 13:00:34 07409496-a423-4a3e-b620-2cfb01a9318d_HyperV-ComputeNetwork.dll
07/12/2019 10:08:37 13/10/2022 9:42:37  69fe178f-26e7-43a9-aa7d-2b616b672dde_eventlogservice.dll
06/09/2022 13:08:54 13/10/2022 9:42:37  6bea57fb-8dfb-4177-9ae8-42e8b3529933_RuntimeDeviceInstall.dll
13/10/2022 9:11:40  13/10/2022 12:37:26 aadauthhelper.dll
13/10/2022 9:11:41  18/10/2022 8:40:22  aadcloudap.dll
06/09/2022 13:07:33 13/10/2022 9:42:37  aadjcsp.dll
13/10/2022 9:11:41  18/10/2022 11:00:20 aadtb.dll
13/10/2022 9:11:40  18/10/2022 11:57:13 aadWamExtension.dll
06/09/2022 13:06:20 13/10/2022 12:40:25 AarSvc.dll
06/09/2022 13:08:52 13/10/2022 9:42:37  AboutSettingsHandlers.dll
21/09/2022 11:05:34 18/10/2022 8:41:06  AboveLockAppHost.dll
09/04/2021 15:57:11 14/10/2022 12:40:35 accessibilitycpl.dll
09/04/2021 15:58:34 18/10/2022 8:42:46  accountaccessor.dll
09/04/2021 15:58:34 13/10/2022 9:42:37  AccountsRt.dll
13/10/2022 9:12:46  13/10/2022 12:37:29 AcGenral.dll
06/09/2022 13:11:03 18/10/2022 11:17:50 AcLayers.dll
07/12/2019 10:09:34 13/10/2022 9:42:37  acledit.dll
07/12/2019 10:09:34 13/10/2022 9:42:37  aclui.dll
06/09/2022 13:07:54 18/10/2022 8:42:18  acmigration.dll
06/09/2022 13:06:49 18/10/2022 8:41:01  ACPBackgroundManagerPolicy.dll
09/04/2021 15:57:11 18/10/2022 11:59:37 acppage.dll
07/12/2019 10:09:37 18/10/2022 10:58:25 acproxy.dll
09/04/2021 15:58:06 18/10/2022 10:35:29 AcSpecfc.dll
```

7.- Muestra el tamaño (*Length*) y nombre completo (*FullName*) de todos los ficheros del directorio ordenados por tamaño en sentido descendente.

```
PS C:\Windows\system32> Get-ChildItem | Select-Object Length, FullName |Sort-Object -descending

  Length FullName
  ------ --------
   17920 C:\Windows\system32\reset.exe
 1257472 C:\Windows\system32\reseteng.dll
  250696 C:\Windows\system32\RESAMPLEDMO.DLL
  113152 C:\Windows\system32\ResBParser.dll
 2430832 C:\Windows\system32\ResetEngine.dll
  110592 C:\Windows\system32\resmon.exe
  528384 C:\Windows\system32\ResourceMapper.dll
   21360 C:\Windows\system32\ResetEngine.exe
  192512 C:\Windows\system32\ResetEngOnline.dll
   74240 C:\Windows\system32\RemoveDeviceContextHandler.dll
   14848 C:\Windows\system32\RemoveDeviceElevated.dll
   63488 C:\Windows\system32\RemoteWipeCSP.dll
   68608 C:\Windows\system32\RemovableMediaProvisioningPlugin.dll
     256 C:\Windows\system32\removerootporterr.mof
   22528 C:\Windows\system32\replace.exe
  123392 C:\Windows\system32\ReportingCSP.dll
    6656 C:\Windows\system32\rendezvousSession.tlb
  129024 C:\Windows\system32\repair-bde.exe
    1091 C:\Windows\system32\RestartTonight_80.png
    1091 C:\Windows\system32\RestartTonight_80_contrast-black.png
     785 C:\Windows\system32\RestartNowPower_80.contrast-white.png
     759 C:\Windows\system32\RestartNowPower_80.png
    1003 C:\Windows\system32\RestartTonight_80_contrast-white.png
  153600 C:\Windows\system32\Ribbons.scr
  612352 C:\Windows\system32\riched20.dll
```

8.- Muestra el tamaño y nombre completo de todos los ficheros del directorio que tengan un tamaño superior a 10MB (10000000 bytes) ordenados por tamaño.

```
PS C:\Windows\system32> Get-ChildItem C:/Windows\System32 | Where-Object Length -gt "10000000" | Select-Object Length, FullName | Sort-Object length -descending

  Length FullName
  ------ --------
147398024 C:\Windows\System32\MRT.exe
 32608744 C:\Windows\System32\WindowsCodecsRaw.dll
 31514312 C:\Windows\System32\nvoglv64.dll
 26268672 C:\Windows\System32\edgehtml.dll
 24272384 C:\Windows\System32\Hydrogen.dll
 23449600 C:\Windows\System32\mshtml.dll
 22992072 C:\Windows\System32\nvcompiler.dll
 18767872 C:\Windows\System32\HoloIgramWorld.dll
 18634264 C:\Windows\System32\nvwgf2umx.dll
 17559432 C:\Windows\System32\nvd3dumx.dll
 17551872 C:\Windows\System32\Windows.UI.Xaml.dll
 14208384 C:\Windows\System32\vmms.exe
 13916600 C:\Windows\System32\nvopencl.dll
 13828032 C:\Windows\System32\nvcuda.dll
 11445248 C:\Windows\System32\wmp.dll
 10846592 C:\Windows\System32\ntoskrnl.exe
 10349360 C:\Windows\System32\Windows.Media.Protection.PlayReady.dll


PS C:\Windows\system32>
```

9.- Muestra el tamaño y nombre completo de todos los ficheros del directorio que tengan un tamaño superior a 10MB y extensión .exe ordenados por tamaño.

```
PS C:\Windows\system32> Get-ChildItem C:/Windows\System32 | Where-Object Length -gt "10000000" | Where-Object Extension -eq .exe | Select-Object Length, FullName | Sort-Object length

   Length FullName
   ------ --------
 10046592 C:\Windows\System32\ntoskrnl.exe
 14208384 C:\Windows\System32\vmms.exe
147398024 C:\Windows\System32\MRT.exe


PS C:\Windows\system32>
```

Hemos visto cómo usar el comando Where-Object para filtrar objetos con propiedades de tipo texto o numérico (por ejemplo, Where-Object CPU -gt 1 o Where-Object Name -eq “Notepad”, sin embargo, hay propiedades que pueden tener otro tipo de datos. Dos de estos datos son los booleanos y los de tipo fecha.

- Las propiedades **booleanas** son las que pueden tener un valor de Verdadero o Falso, por ejemplo, la propiedad Exists del comando Get-ChildItem.

```
DirectoryName                Property        string DirectoryName {get
Exists                       Property        bool Exists {get;}
Extension                    Property        string Extension {get;}
```

  Cuando queremos filtrar por estas propiedades y queremos poner que un valor es verdadero o falso, no podemos poner directamente True o False, ya que el sistema las interpretará como cadenas de texto en lugar de hacerlo como valores booleanos. En estos casos, es necesario utilizar dos variables del sistema que representaremos de la forma **$True** y **$False**.
- Otro tipo de propiedades muy común son las de fecha y hora, que podemos encontrar por ejemplo en la fecha de creación de un fichero.

```
PS C:\Users\victor> Get-ChildItem | Get-Member CreationTime

   TypeName: System.IO.DirectoryInfo

Name         MemberType Definition
----         ---------- ----------
CreationTime Property   datetime CreationTime {get;set;}
```

- Aquí encontramos el mismo problema que en el caso anterior ya que si ponemos la fecha directamente la interpretará como una cadena. En este caso, hay que utilizar el comando **Get-Date** con el parámetro **-date** que convierte una fecha en modo texto a un objeto de tipo datetime que almacena dicha fecha.

```
PS C:\Users\victor> get-date -date "2 de noviembre de 2021"

martes, 2 de noviembre de 2021 0:00:00
```

  Pero ahora hay otro problema, ¿cómo hacemos para incluir el valor devuelto por este comando en el parámetro de otro comando? En este caso tenemos que recurrir a los paréntesis de la siguiente forma:

```
PS C:\Users\victor> Get-ChildItem | Where-Object CreationTime -gt (Get-Date -date "1 de octubre de 2021")
```

  Los **paréntesis** hacen que en primer lugar se ejecute el comando que hay en su interior y, el valor devuelto por dicho comando reemplazará todo lo que hay entre paréntesis.

Hay diversas formas de indicar la fecha que se le pasa al comando Get-Date, tanto con fecha y hora como solo fecha. Algunos ejemplos son:

- “2 de noviembre de 2021 10:05:00”
- “02/11/2021”
- “02/11/21 10:10:30”
- “2021-02-11”

Teniendo en cuenta lo anterior, realiza los siguientes ejercicios:

10.- Muestra todos los procesos que tienen el estado Respond puesto a False, es decir, todos los procesos del sistema que se hayan colgado.

```
PS C:\Windows\system32> Get-Process | Where-Object Responding -eq $false

Handles  NPM(K)    PM(K)      WS(K)     CPU(s)      Id  SI ProcessName
-------  ------    -----      -----     ------      --  -- -----------
    699      36    35460       1612       0,50   6788   1 SystemSettings
```

11.- Muestra todos los ficheros de C:\Windows que hayan sido creados con fecha posterior al 15 de octubre.

```
PS C:\Windows\system32> Get-ChildItem |Where-Object CreationTime -gt  "15/10/2022 13:32:06".date


    Directorio: C:\Windows\system32


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        07/12/2019     15:55                0409
d-----        09/04/2021     16:02                AdvancedInstallers
d-----        07/12/2019     10:14                am-et
d-----        07/12/2019     10:14                AppLocker
d-----        06/09/2022     13:31                appraiser
d---s-        06/09/2022     13:31                AppV
d-----        06/09/2022     13:31                ar-SA
d-----        27/09/2022     13:00                BestPractices
d-----        06/09/2022     13:31                bg-BG
d-----        13/10/2022     12:36                Boot
d-----        07/12/2019     10:14                Bthprops
d-----        06/09/2021     11:54                CatRoot
d-----        13/10/2022     12:37                catroot2
d-----        06/09/2022     13:31                CodeIntegrity
d-----        09/04/2021     16:02                Com
d-----        18/10/2022      9:35                config
d---s-        07/12/2019     10:31                Configuration
d-----        07/12/2019     10:14                ContainerSettingsProviders
d-----        06/09/2022     13:31                cs-CZ
d-----        06/09/2022     13:31                da-DK
d-----        22/09/2022      8:46                DDFs
d-----        06/09/2022     13:31                de-DE
d---s-        06/09/2022     13:31                DiagSvcs
d-----        13/10/2022     12:36                Dism
d-----        07/12/2019     10:14                downlevel
d-----        13/10/2022     12:36                drivers
```