Carla García Parra 2ºASIR

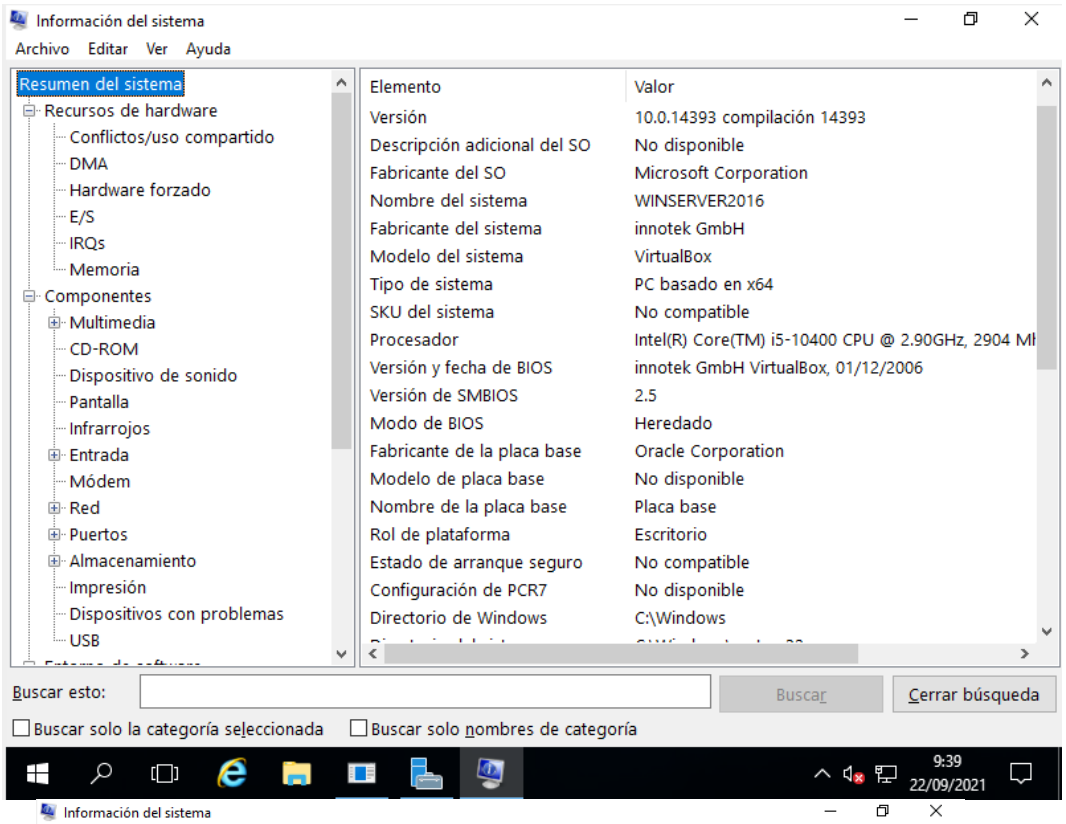
Tarea 3

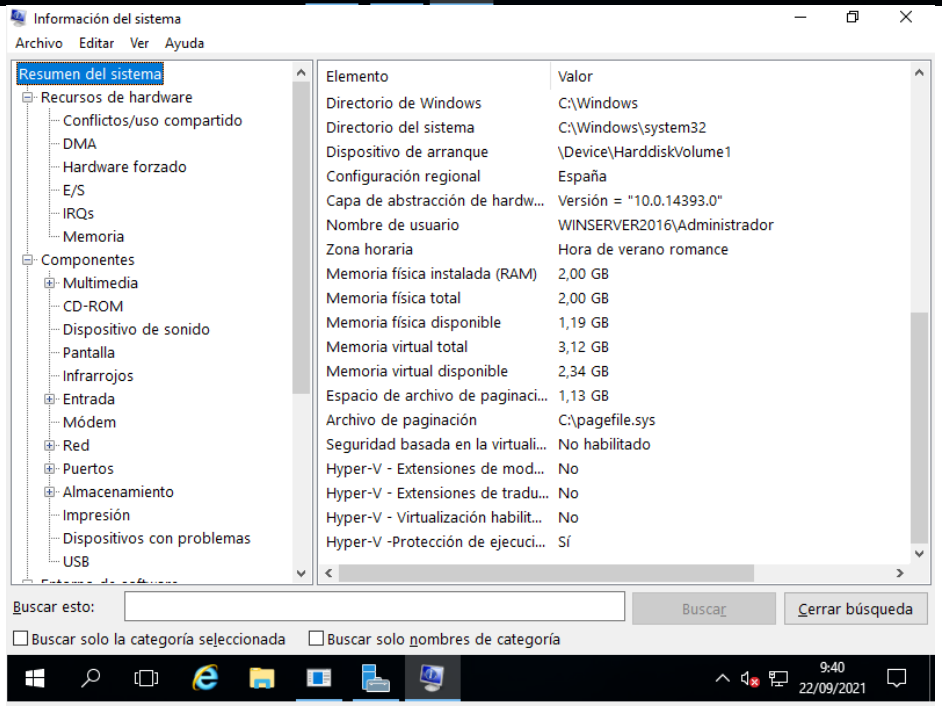
Buscar información del sistema operativo de la máquina virtuale Windows Server 2016.

1. Interfaz gráfica de Windows server 2016. Realizar una breve descripción de los dispositivos de la máquina.

MSINFO32.EXE

Tenemos un sistema windows 2016 versión 10.0.14393 con procesador intel core i5 y 4gb de memoria RAM





2. Consola (CMD administrador) de Windows server 2016.

- Utilizar todos los comandos que se describen en la siguiente dirección y guardar todos los resultados en un fichero llamado filesystem.txt
  - Comando systeminfo → listado con la información del sistema

```
C:\Users\Administrador.WIN-V0LV1BK8OEB\Documents>systeminfo > filesystem.txt

C:\Users\Administrador.WIN-V0LV1BK8OEB\Documents>dir
 El volumen de la unidad C no tiene etiqueta.
 El número de serie del volumen es: D6C3-80C0

 Directorio de C:\Users\Administrador.WIN-V0LV1BK8OEB\Documents

22/09/2021  09:52    <DIR>          .
22/09/2021  09:52    <DIR>          ..
22/09/2021  09:52             3.127 filesystem.txt
15/03/2020  20:20    <DIR>          WindowsPowerShell
               1 archivos          3.127 bytes
               3 dirs  37.012.025.344 bytes libres

C:\Users\Administrador.WIN-V0LV1BK8OEB\Documents>
```

```
Administrador: Símbolo del sistema
C:\Users\Administrador.WIN-V0LV1BK8OEB\Documents>type filesystem.txt

Nombre de host:                           WINSERVER2016
Nombre del sistema operativo:             Microsoft Windows Server 2016 Datacenter
Versión del sistema operativo:            10.0.14393 N/D Compilación 14393
Fabricante del sistema operativo:         Microsoft Corporation
Configuración del sistema operativo:      Servidor independiente
Tipo de compilación del sistema operativo: Multiprocessor Free
Propiedad de:                             Usuario de Windows
Organización registrada:
Id. del producto:                         00376-40000-00000-AA947
Fecha de instalación original:            29/10/2018, 18:27:21
Tiempo de arranque del sistema:           22/09/2021, 9:38:02
Fabricante del sistema:                   innotek GmbH
Modelo el sistema:                        VirtualBox
Tipo de sistema:                          x64-based PC
Procesador(es):                           1 Procesadores instalados.
                                          [01]: Intel64 Family 6 Model 165 Stepping 3 GenuineInt
el ~2904 Mhz
Versión del BIOS:                         innotek GmbH VirtualBox, 01/12/2006
Directorio de Windows:                    C:\Windows
Directorio de sistema:                    C:\Windows\system32
Dispositivo de arranque:                  \Device\HarddiskVolume1
Configuración regional del sistema:       es;Español (internacional)
Idioma de entrada:                        es;Español (tradicional)
Zona horaria:                             (UTC+01:00) Bruselas, Copenhague, Madrid, París
Cantidad total de memoria física:         2.048 MB
Memoria física disponible:                1.096 MB
Memoria virtual: tamaño máximo:           3.200 MB
Memoria virtual: disponible:              2.250 MB
Memoria virtual: en uso:                  950 MB
Ubicación(es) de archivo de paginación:   C:\pagefile.sys
Dominio:                                  AVELLANEDA
```

- Muestra o establece la hora del sistema

```
C:\Users\Administrador.WIN-V0LV1BK8OEB\Documents>time >> filesystem.txt
```

```
                                      Servidor DHCP:      10.1.0.1
                                      Direcciones IP
                                      [01]: 10.1.1.9
                                      [02]: fe80::84f7:d7da:95f:7809
Requisitos Hyper-V:                 Extensiones de modo de monitor de VM: No
                                    Se habilitó la virtualización en el firmware: No
                                    Traducción de direcciones de segundo nivel: No
                                    La prevención de ejecución de datos está disponible: Sí
La hora actual es:  9:57:27,42
```

- Muestra la version de Windows

```
C:\Users\Administrador.WIN-V0LV1BK8OEB\Documents>ver

Microsoft Windows [Versión 10.0.14393]

C:\Users\Administrador.WIN-V0LV1BK8OEB\Documents>ver >> filesystem.txt

C:\Users\Administrador.WIN-V0LV1BK8OEB\Documents>type filesystem.txt
```

- Para obtener un listado completo de todos los procesos que se encuentran en el sistema

```
C:\Users\Administrador.WIN-V0LV1BK8OEB\Documents>tasklist >> filesystem.txt
```

```
Microsoft Windows [Versión 10.0.14393]

Nombre de imagen              PID Nombre de sesión Núm. de ses Uso de memor
========================= ======== ================ =========== ============
System Idle Process             0 Services                   0          4 KB
System                          4 Services                   0        140 KB
smss.exe                      288 Services                   0      1.212 KB
csrss.exe                     360 Services                   0      4.160 KB
wininit.exe                   428 Services                   0      5.140 KB
csrss.exe                     436 Console                    1      7.592 KB
winlogon.exe                  484 Console                    1      9.076 KB
services.exe                  552 Services                   0      6.728 KB
lsass.exe                     560 Services                   0     13.588 KB
svchost.exe                   640 Services                   0     18.728 KB
svchost.exe                   700 Services                   0      8.796 KB
dwm.exe                       800 Console                    1     44.672 KB
svchost.exe                   848 Services                   0     44.792 KB
svchost.exe                   912 Services                   0     21.452 KB
svchost.exe                   952 Services                   0     17.332 KB
svchost.exe                   960 Services                   0     23.452 KB
svchost.exe                   356 Services                   0     19.816 KB
svchost.exe                  1056 Services                   0     24.792 KB
svchost.exe                  1216 Services                   0      6.784 KB
spoolsv.exe                  1464 Services                   0     15.316 KB
svchost.exe                  1516 Services                   0     19.632 KB
svchost.exe                  1536 Services                   0      8.044 KB
MsMpEng.exe                  1588 Services                   0    130.804 KB
svchost.exe                  1624 Services                   0     16.212 KB
RuntimeBroker.exe            2528 Console                    1     20.188 KB
```

- Comando driverquery que nos muestra una lista de los controladores de dispositivos que tenemos instalados en nuestro sistema

```
C:\Users\Administrador.WIN-V0LV1BK8OEB\Documents>driverquery >> filesystem.txt
```

```
C:\Users\Administrador.WIN-V0LV1BK8OEB\Documents>driverquery

Nombre módu. Nombre para mostrar    Tipo control. Fecha de vínculo
============ ===================== ============= ====================
1394ohci     Controladora de host c Kernel        16/07/2016 4:21:36
3ware        3ware                 Kernel        19/05/2015 0:28:03
ACPI         Controlador Microsoft  Kernel        16/07/2016 4:10:47
AcpiDev      Controlador de disposi Kernel        16/07/2016 4:29:10
acpiex       Microsoft ACPIEx Drive Kernel        16/07/2016 4:28:23
acpipagr     Controlador de agregad Kernel        16/07/2016 4:29:00
AcpiPmi      Controlador de medidor Kernel        16/07/2016 4:19:44
acpitime     Controlador de alarma  Kernel        16/07/2016 4:29:20
ADP80XX      ADP80XX               Kernel        09/04/2015 22:49:48
AFD          Controlador de función Kernel        16/07/2016 4:24:31
ahcache      Application Compatibil Kernel        16/07/2016 4:10:40
AmdK8        Controlador de procesa Kernel        16/07/2016 4:10:42
AmdPPM       Controlador de procesa Kernel        16/07/2016 4:10:41
amdsata      amdsata               Kernel        14/05/2015 14:14:52
amdsbs       amdsbs                Kernel        11/12/2012 22:21:44
amdxata      amdxata               Kernel        01/05/2015 2:55:35
AppID        Controlador de AppId   Kernel        16/07/2016 4:27:05
applockerflt Controlador de filtro  Kernel        16/07/2016 4:27:27
AppvStrm     AppvStrm              File System   16/07/2016 4:10:45
AppvVemgr    AppvVemgr             File System   16/07/2016 4:10:56
AppvVfs      AppvVfs               File System   16/07/2016 4:10:53
arcsas       Controlador de minipue Kernel        09/04/2015 21:12:07
AsyncMac     Controlador de medios  Kernel        16/07/2016 4:29:00
atapi        Canal IDE             Kernel        16/07/2016 4:29:05
b06bdrv      Adaptador VBD de red Q Kernel        25/05/2016 9:03:08
BasicDisplay BasicDisplay          Kernel        16/07/2016 4:28:02
BasicRender  BasicRender           Kernel        16/07/2016 4:28:14
bcmfn        bcmfn Service         Kernel        08/06/2015 10:32:02
bcmfn2       bcmfn2 Service        Kernel        16/03/2014 11:07:36
Beep         Beep                  Kernel        16/07/2016 4:22:02
```

- Mostrar el contenido del fichero filesystem.txt página a página.

```
C:\Users\Administrador.WIN-V0LV1BK8OEB\Documents>more filesystem.txt
```

Con este comando te saldrá paginado el txt, dándole al espacio

- Mostrar las líneas numeradas del fichero filesystem.txt que contengan la palabra “Memoria” y guardar las líneas en un fichero llamado FilesystemMemoria.txt

```
C:\Users\Administrador.WIN-V0LV1BK8OEB\Documents>find /N "Memoria" filesystem.txt

---------- FILESYSTEM.TXT
[26]Memoria física disponible:               1.096 MB
[27]Memoria virtual: tamaño máximo:          3.200 MB
[28]Memoria virtual: disponible:             2.250 MB
[29]Memoria virtual: en uso:                 950 MB

C:\Users\Administrador.WIN-V0LV1BK8OEB\Documents>find /N "Memoria" filesystem.txt > filesystemMemoria.txt
```

- Borrar los ficheros filesystem.txt y FilesystemMemoria.txt

```
C:\Users\Administrador.WIN-V0LV1BK8OEB\Documents>del filesystem.txt

C:\Users\Administrador.WIN-V0LV1BK8OEB\Documents>del filesystemMemoria.txt

C:\Users\Administrador.WIN-V0LV1BK8OEB\Documents>dir
 El volumen de la unidad C no tiene etiqueta.
 El número de serie del volumen es: D6C3-80C0

 Directorio de C:\Users\Administrador.WIN-V0LV1BK8OEB\Documents

22/09/2021  10:28    <DIR>          .
22/09/2021  10:28    <DIR>          ..
15/03/2020  20:20    <DIR>          WindowsPowerShell
               0 archivos              0 bytes
               3 dirs  36.999.245.824 bytes libres
```

3. PowerShell Windows server 2016

- Leer el artículo de la siguiente dirección: https://esgeeks.com/como-usar-windows-powershell-guia-basica/
- Arrancar PowerShell con la consola de Windows server 2016

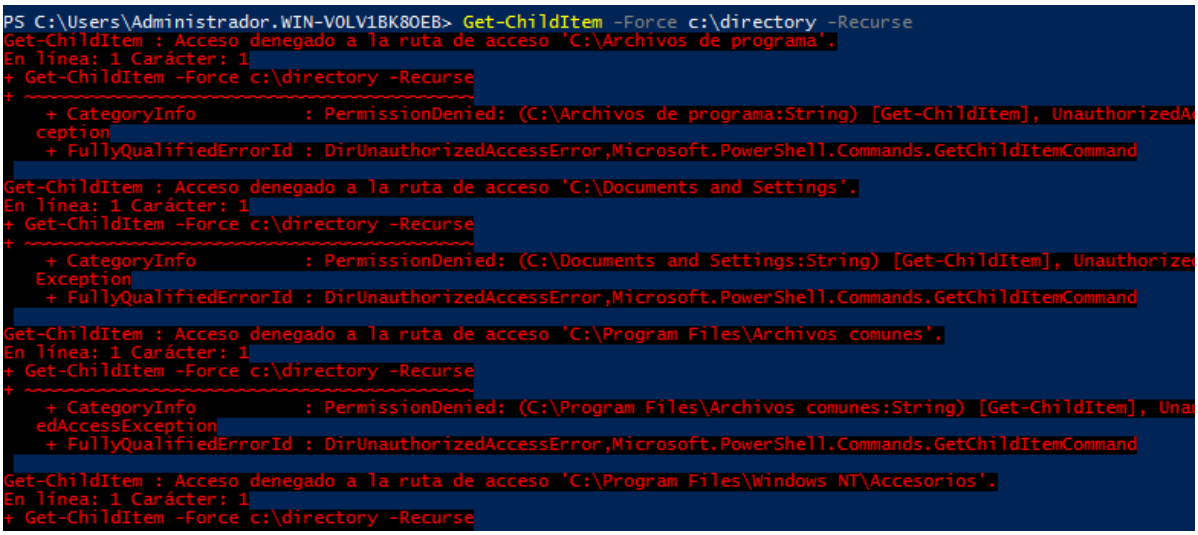
```
C:\Users\Administrador.WIN-V0LV1BK8OEB\Documents>powershell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. Todos los derechos reservados.

PS C:\Users\Administrador.WIN-V0LV1BK8OEB\Documents> _
```

- Ejecutar todos los comandos que se enumeran en la siguiente dirección, haciendo una breve descripción de la acción que realizan.
  https://searchdatacenter.techtarget.com/es/consejo/25-principales-comandos-de-Windows-PowerShell-para-administradores
  NOTA: Dependiendo de la versión de PowerShell que se utilice puede variar algún atributo.

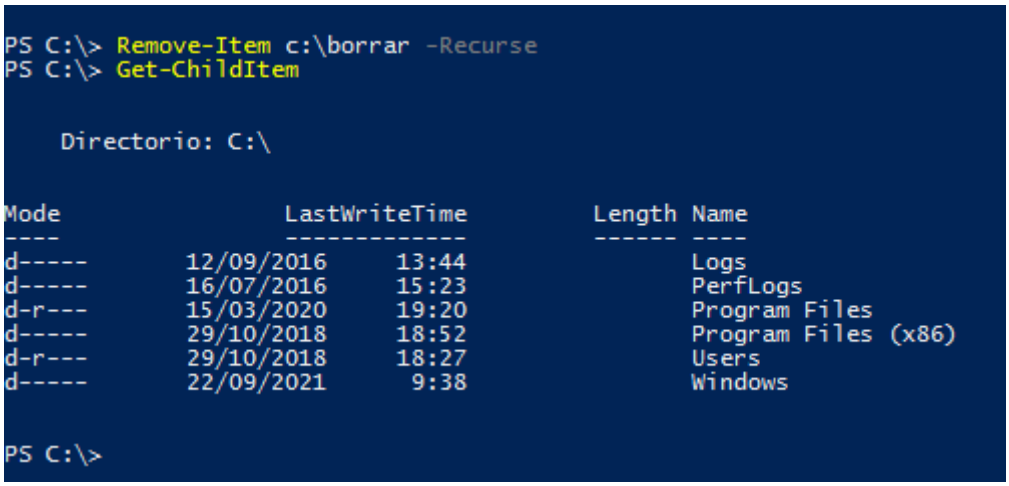
  - Liste todos los elementos dentro de una carpeta

```
PS C:\Users\Administrador.WIN-V0LV1BK8OEB> Get-ChildItem -Force


    Directorio: C:\Users\Administrador.WIN-V0LV1BK8OEB


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d--h--        29/10/2018     18:27                AppData
d--hsl        29/10/2018     18:27                Configuración local
d-r---        29/10/2018     18:28                Contacts
d--hsl        29/10/2018     18:27                Cookies
d--hsl        29/10/2018     18:27                Datos de programa
d-r---        29/10/2018     18:28                Desktop
d-r---        22/09/2021     10:28                Documents
d-r---        04/11/2018     12:40                Downloads
d--hsl        29/10/2018     18:27                Entorno de red
d-r---        29/10/2018     18:28                Favorites
d--hsl        29/10/2018     18:27                Impresoras
d-r---        29/10/2018     18:28                Links
d--hsl        29/10/2018     18:27                Menú Inicio
d--hsl        29/10/2018     18:27                Mis documentos
d-r---        29/10/2018     18:28                Music
d-r---        29/10/2018     18:28                Pictures
d--hsl        29/10/2018     18:27                Plantillas
d--hsl        29/10/2018     18:27                Reciente
d-r---        29/10/2018     18:28                Saved Games
d-r---        29/10/2018     18:28                Searches
d--hsl        29/10/2018     18:27                SendTo
d-r---        29/10/2018     18:28                Videos
-a-h--        15/03/2020     19:32         786432 NTUSER.DAT
-a-hs-        29/10/2018     18:27          45056 ntuser.dat.LOG1
-a-hs-        29/10/2018     18:27          24576 ntuser.dat.LOG2
-a-hs-        22/09/2021      9:38              0 NTUSER.DAT{f5c305a3-789a-11e6-afef-c1c1994789
                                                   0a}.TxR.0.regtrans-ms
```

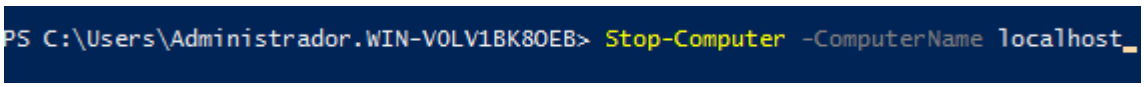
- Recurra sobre una serie de directorios o carpetas



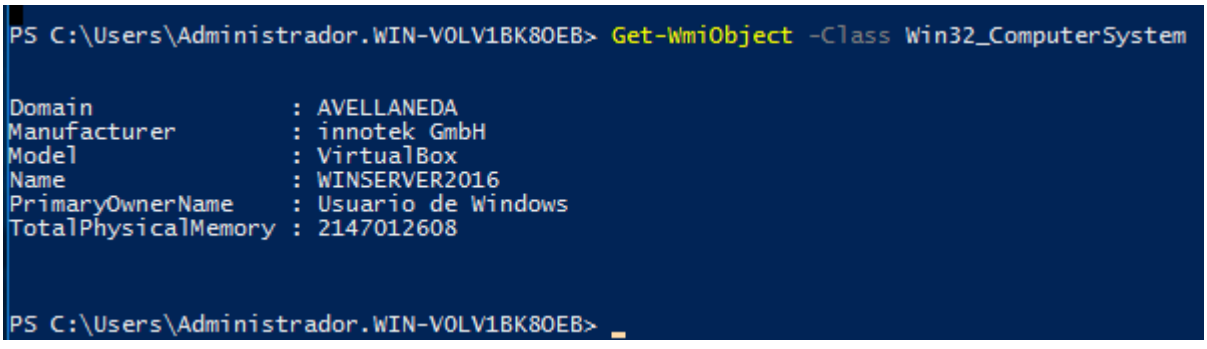
- Elimine todos los archivos dentro de un directorio o carpetas



- Reinicie la computadora actual



- Obtener información sobre la fabricación y modelo de una computadora



- Obtener información sobre la BIOS de la computadora actual

```
PS C:\Users\Administrador.WIN-VOLV1BK8OEB> Get-WmiObject -Class Win32_BIOS -Computername winserver2016


SMBIOSBIOSVersion : VirtualBox
Manufacturer      : innotek GmbH
Name              : Default System BIOS
SerialNumber      : 0
Version           : VBOX   - 1


PS C:\Users\Administrador.WIN-VOLV1BK8OEB> _
```

- Lista de arreglos en caliente instalados

```
PS C:\Users\Administrador.WIN-VOLV1BK8OEB> Get-WmiObject -Class Win32_QuickFixEngineering -Computername winse

Source        Description      HotFixID      InstalledBy          InstalledOn
------        -----------      --------      -----------          -----------
WINSERVER2016 Update           KB3192137     NT AUTHORITY\SYSTEM  12/09/2016 0:00:00


PS C:\Users\Administrador.WIN-VOLV1BK8OEB> _
```

- Obtenga el nombre de usuario de la persona actualmente registrada en la computadora

```
PS C:\Users\Administrador.WIN-VOLV1BK8OEB> Get-WmiObject -Class Win32_ComputerSystem -Property UserName -Computername wi
nserver2016


__GENUS          : 2
__CLASS          : Win32_ComputerSystem
__SUPERCLASS     :
__DYNASTY        :
__RELPATH        :
__PROPERTY_COUNT : 1
__DERIVATION     : {}
__SERVER         :
__NAMESPACE      :
__PATH           :
UserName         : WINSERVER2016\Administrador
PSComputerName   :


PS C:\Users\Administrador.WIN-VOLV1BK8OEB> _
```

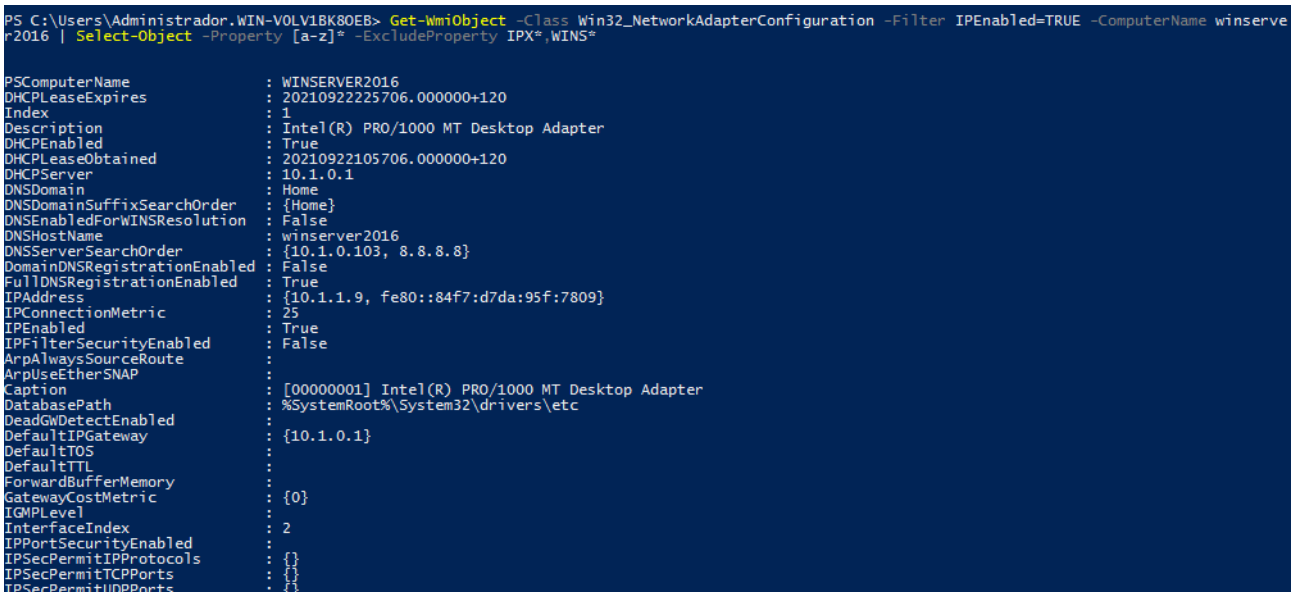
- Encuentre solo los nombres de las aplicaciones instaladas en la computadora actual

```
PS C:\Users\Administrador.WIN-VOLV1BK8OEB> Get-WmiObject -Class Win32_Product -Computername winserver2016 | Format-Wide -Column 1
PS C:\Users\Administrador.WIN-VOLV1BK8OEB>
```

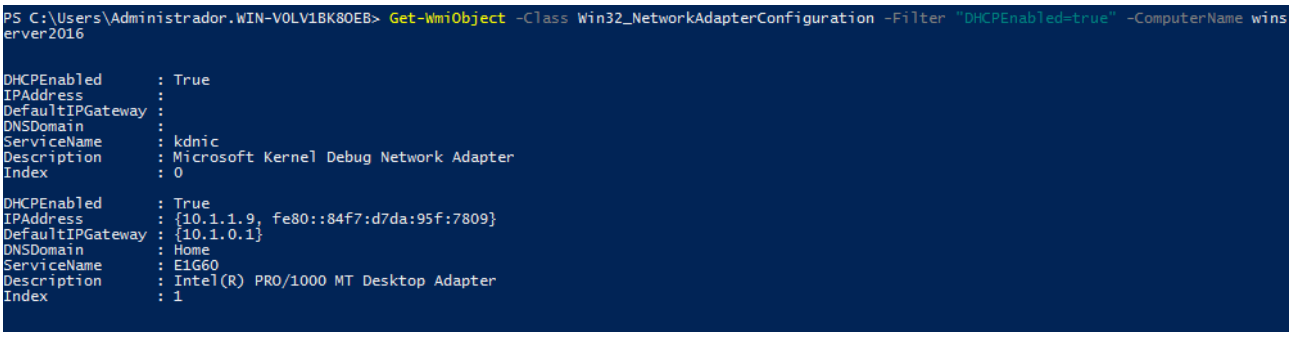
- Obtenga direcciones IP asignadas a la computadora actualmente

```
PS C:\Users\Administrador.WIN-VOLV1BK8OEB> Get-WmiObject -Class Win32_NetworkAdapterConfiguration -Filter IPEnabled=TRUE -ComputerName winserve
r2016 | Format-table -Property IPAddress

IPAddress
---------
{10.1.1.9, fe80::84f7:d7da:95f:7809}
```

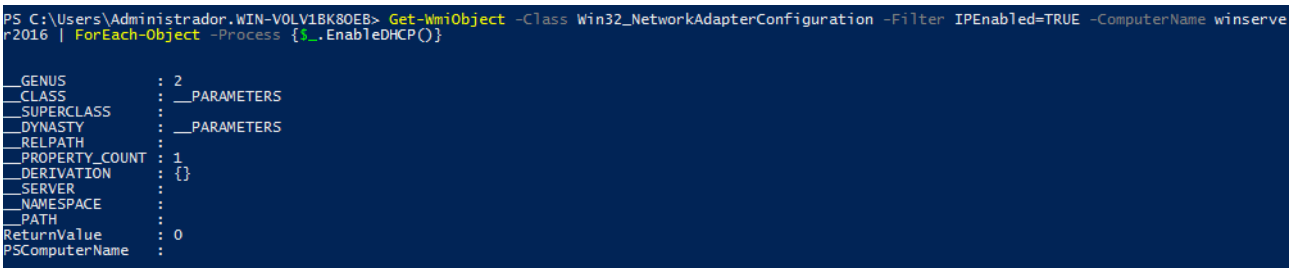
- Obtenga un reporte de configuraciones Ip más detallada para la máquina virtual



- Encuentre las tarjetas de red con DHCP habilitado en la computadora actualmente



- Habilite DHCP en todos los adaptadores de red en la computadora actualmente



- Remotamente apague otra máquina después de un minuto