

Práctica de laboratorio: Utilizar Windows PowerShell

NOTA: RESPONDER CADA PREGUNTA CON CAPTURAS DE PANTALLA COMPLETAS DONDE SE VEAN LAS SIGLAS DE SU NOMBRE AL LADO DEL RELOJ. EN LUGAR DE COLOCAR UN TEXTO DEBE DE SELECCIONAR EL TEXTO INVESTIGADO EN UNA PÁGINA WEB Y HACERLE CAPTURA DE PANTALLA COMPLETA, PARA LUEGO COLOCARLA AQUÍ. SI SON VARIAS PREGUNTAS, DEBE COLOCAR VARIAS CAPTURAS DE PANTALLAS COMPLETAS. NO COLOCAR INFORMACIÓN ENCONTRADA EN NETACAD, COLOCAR INFORMACIÓN INVESTIGADA EN OTRAS PÁGINAS WEB O LO REALIZADO POR USTED.

Objetivos

El objetivo de esta práctica de laboratorio es estudiar algunas de las funciones de PowerShell.

Parte 1: Acceder a la consola PowerShell.

Parte 2: Explorar los comandos del Command Prompt y del PowerShell.

Parte 3: Explorar cmdlets.

Parte 4: Explorar el comando netstat utilizando PowerShell.

Parte 5: Vaciar la papelera de reciclaje utilizando PowerShell

Antecedentes / Escenario

PowerShell es una potente herramienta de automatización. Es una consola de comandos, y también un lenguaje de scripts. En esta práctica de laboratorio utilizarán la consola para ejecutar algunos de los comandos disponibles tanto en el símbolo del sistema como en PowerShell. PowerShell también tiene funciones que pueden crear scripts para automatizar tareas y trabajar junto con el Sistema operativo Windows.

Recursos necesarios

- 1 PC Windows con PowerShell instalado y acceso a internet

Instrucciones

Parte 1: Acceso a la consola de PowerShell.

- a. Hagan clic en **Inicio**. Busquen y seleccionen **powershell**.
 - b. Hagan clic en **Inicio**. Busquen y seleccionen el **símbolo del sistema**.

Parte 2: Estudien los comandos del símbolo del sistema y de PowerShell.

- a. Introduzcan **dir** en los cursores de ambas ventanas.

```
Windows PowerShell x + - C:\WINDOWS\system32\cmd. x - + - PS C:\Users\msi2> dir

Directorio: C:\Users\msi2

Mode LastWriteTime Length Name
---- -- -- -- -
d----- 10/10/2025 2:41 p. m. AL .cache
d----- 10/10/2025 2:42 p. m. AL .dotnet
d----- 10/10/2025 2:41 p. m. AL .nuget
d----- 21/7/2025 5:56 p. m. AL .redhat
d----- 10/10/2025 2:34 p. m. AL .templateengine
d----- 21/10/2025 7:36 p. m. AL .VirtualBox
d----- u/7/2025 11:00 p. m. AL .vscode
d----- 23/7/2025 4:09 p. m. AL .zenvmap
d----- 19/2/2025 4:18 p. m. AL ansel
d----- 21/10/2025 7:35 p. m. AL Cisco Packet Tracer 8.2.2
d----- 5/4/2025 2:00 p. m. AL Contacts
d----- 10/10/2025 1:52 p. m. AL Documents
d----- 24/10/2025 1:36 p. m. AL Downloads
d----- 5/4/2025 2:00 p. m. AL Favorites
d----- 5/4/2025 2:00 p. m. AL Links
d----- 5/4/2025 2:00 p. m. AL Music
d----- 5/4/2025 2:00 p. m. AL OneDrive
d----- 9/10/2025 3:37 p. m. AL pseint
d----- 9/6/2025 9:46 a. m. AL Saved Games
d----- 5/4/2025 2:00 p. m. AL Searches
d----- 5/4/2025 2:00 p. m. AL source
d----- 10/10/2025 2:41 p. m. AL Videos
d----- 23/10/2025 11:29 p. m. AL VirtualBox VMs
d----- 20/10/2025 11:55 p. m. AL
d----- 9/7/2025 7:12 p. m. AL 188._gitconfig
d----- 21/10/2025 7:24 p. m. AL 174._packettracer
d----- 11/3/2025 12:06 a. m. AL 49969.Hoja de presentación[1].docx
-a--- 5/4/2025 3:26 a. m. AL 57287.Hoja de presentación[1].pdf
-a--- 14/7/2025 6:26 p. m. AL 3453.olimpico
-a--- 7/5/2025 6:48 p. m. AL 527.psc
-a--- 11/3/2025 12:02 a. m. AL 57275.razonamiento.pdf

C:\Users\msi2>dir

El volumen de la unidad C es Windows
El número de serie del volumen es: DC5A-0FD5

Directorio de C:\Users\msi2

21/10/2025 05:03 p. m. AL <DIR> .
22/10/2025 06:33 p. m. AL <DIR> ..
10/10/2025 02:41 p. m. AL <DIR> .cache
10/10/2025 02:42 p. m. AL <DIR> .dotnet
09/07/2025 07:12 p. m. AL <DIR> 188._gitconfig
10/10/2025 02:41 p. m. AL <DIR> .nuget
21/10/2025 07:24 p. m. AL <DIR> 174._packettracer
21/07/2025 05:56 p. m. AL <DIR> .redhat
10/10/2025 02:34 p. m. AL <DIR> .templateengine
21/10/2025 07:36 p. m. AL <DIR> .VirtualBox
04/07/2025 11:00 p. m. AL <DIR> .vscode
04/07/2025 09:40 p. m. AL <DIR> .zenvmap
19/03/2025 04:10 p. m. AL <DIR> ansel
21/10/2025 07:31 p. m. AL <DIR> Cisco Packet Tracer 8.2.2
05/04/2025 02:00 p. m. AL <DIR> Contacts
05/04/2025 01:52 p. m. AL <DIR> Documents
05/04/2025 02:00 p. m. AL <DIR> Downloads
05/04/2025 01:36 p. m. AL <DIR> Favorites
05/04/2025 02:00 p. m. AL <DIR> Links
05/04/2025 01:36 a. m. AL <DIR> Music
05/04/2025 02:00 p. m. AL <DIR> OneDrive
05/04/2025 02:00 p. m. AL <DIR> Favorites
11/03/2025 12:06 a. m. AL 49,969.Hoja de presentación[1].docx
05/04/2025 03:26 a. m. AL 57,207.Hoja de presentación[1].pdf
05/04/2025 02:00 p. m. AL <DIR> Links
05/04/2025 02:00 p. m. AL <DIR> Music
04/07/2025 06:26 p. m. AL 3,453.olimpico
10/09/2025 03:37 p. m. AL <DIR> OneDrive
07/05/2025 06:48 p. m. AL 527.psc
09/06/2025 09:46 a. m. AL <DIR> pseint
05/04/2025 02:00 p. m. AL <DIR> Saved Games
05/04/2025 02:00 p. m. AL <DIR> Searches
10/10/2025 02:41 p. m. AL <DIR> source
23/10/2025 11:29 p. m. AL <DIR> Videos
20/10/2025 11:55 p. m. AL <DIR> VirtualBox VMs
7 archivos 168,793 bytes
25 dirs 361,659,310,080 bytes libres
```

¿Qué salidas arroja el comando **dir**?

lista los archivos y carpetas del directorio actual

- b. Prueben otro comando que hayan utilizando en el símbolo del sistema, como ping, cd o ipconfig.

```
-a---- 7/5/2025 6:40 p. m. AL      527 p.psc  
-a---- 11/3/2025 12:02 a. m. AL    57275 razonamiento.pdf  
  
PS C:\Users\msi12> ipconfig /all  
  
Configuración IP de Windows  
  
  Nombre de host . . . . . : Alan13  
  Sufijo DNS principal . . . . . :  
  Tipo de nodo . . . . . : híbrido  
  Enrutamiento IP habilitado . . . . : no  
  Proxy WINS habilitado . . . . : no  
  
Adaptador de Ethernet Ethernet 3:  
  
  Sufijo DNS específico para la conexión . . . . . :  
  Descripción . . . . . : VirtualBox Host-Only Ethernet Adapter  
  Dirección física . . . . . : 0A-00-27-00-00-04  
  DHCP habilitado . . . . . : sí  
  Configuración automática habilitada . . . . . : sí  
  Vinculo: dirección IPv6 local . . . . . : fe00::ff2f:b18d:5f48:3601%4(Preferido)  
o)  Dirección IPv4 . . . . . : 192.168.56.1(Preferido)  
  Máscara de subred . . . . . : 255.255.255.0  
  Puerta de enlace predeterminada . . . . . : 772407335  
  IAIID DHCPv6 . . . . . : 00-01-00-01-2E-AC-FD-77-D8-43  
  DUID de cliente DHCPv6 . . . . . : -AE-31-31-D4  
  NetBIOS sobre TCP/IP . . . . . : habilitado  
  
Adaptador de LAN inalámbrica Conexión de área local* 1:  
  
  Estado de los medios . . . . . : medios desconectados  
  Sufijo DNS específico para la conexión . . . . . : Microsoft Wi-Fi Direct Virtua  
l Adapter  
  Descripción . . . . . :  
  Dirección física . . . . . : 28-C5-D2-02-F2-D4  
  DHCP habilitado . . . . . : sí  
  Configuración automática habilitada . . . . . : sí  
  
Adaptador de LAN inalámbrica Conexión de área local* 2:  
  
C:\WINDOWS\system32\cmd . . . . . +  
25 dirs 361,659,310,080 bytes libres  
C:\Users\msi12>ipconfig /all  
  
Configuración IP de Windows  
  
  Nombre de host . . . . . : Alan13  
  Sufijo DNS principal . . . . . :  
  Tipo de nodo . . . . . : híbrido  
  Enrutamiento IP habilitado . . . . : no  
  Proxy WINS habilitado . . . . : no  
  
Adaptador de Ethernet Ethernet 3:  
  
  Sufijo DNS específico para la conexión . . . . . : VirtualBox Host-Only Ethernet Adapter  
  Dirección física . . . . . : 0A-00-27-00-00-04  
  DHCP habilitado . . . . . : no  
  Configuración automática habilitada . . . . . : sí  
  Vinculo: dirección IPv6 local . . . . . : fe00::ff2f:b18d:5f48:3601%4(Preferido)  
o)  Dirección IPv4 . . . . . : 192.168.56.1(Preferido)  
  Máscara de subred . . . . . : 255.255.255.0  
  Puerta de enlace predeterminada . . . . . : 772407335  
  IAIID DHCPv6 . . . . . : 00-01-00-01-2E-AC-FD-77-D8-43  
  DUID de cliente DHCPv6 . . . . . : -AE-31-31-D4  
  NetBIOS sobre TCP/IP . . . . . : habilitado  
  
Adaptador de LAN inalámbrica Conexión de área local* 1:  
  
  Estado de los medios . . . . . : medios desconectados  
  Sufijo DNS específico para la conexión . . . . . : Microsoft Wi-Fi Direct Virtua  
l Adapter  
  Descripción . . . . . :  
  Dirección física . . . . . : 28-C5-D2-02-F2-D4  
  DHCP habilitado . . . . . : sí  
  Configuración automática habilitada . . . . . : sí  
  
Adaptador de LAN inalámbrica Conexión de área local* 2:
```

The screenshot shows two side-by-side command-line interfaces. The left window is a Windows PowerShell session (PS) and the right is a standard cmd session.

Windows PowerShell Session (Left):

```

Servidor DHCP . . . . . : 10.0.0.1
IAID DHCPv6 . . . . . : 170444242
DUID de cliente DHCPv6 . . . . . : 00-01-00-01-2E-AC-FD-77-D8-43
-AE-31-31-D4
Servidores DNS . . . . . :
    10.0.0.1 : fe80::1%18
    fe80::1%18
NetBIOS sobre TCP/IP. . . . . : habilitado

Adaptador de Ethernet Conexión de red Bluetooth:
Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . . . . :
Descripción . . . . . : Bluetooth Device (Personal Area Network)
Dirección física. . . . . : 28-C5-D2-02-F2-D7
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . . . : sí

Adaptador de Ethernet Ethernet 2:
Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . . . . :
Descripción . . . . . : Realtek PCIe GbE Family Controller #2
Dirección física. . . . . : D8-43-AE-31-31-D4
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . . . : sí

PS C:\Users\msi2> ping 8.8.8.8

Haciendo ping a 8.8.8.8 con 32 bytes de datos:
Respueta desde 8.8.8.8: bytes=32 tiempo=35ms TTL=118
Respueta desde 8.8.8.8: bytes=32 tiempo=43ms TTL=118
Respueta desde 8.8.8.8: bytes=32 tiempo=34ms TTL=118
Respueta desde 8.8.8.8: bytes=32 tiempo=38ms TTL=118

Estadísticas de ping para 8.8.8.8:
Paquetes: enviados = 4, recibidos = 4, perdidos = 0
(0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 34ms, Máximo = 43ms, Media = 37ms
PS C:\Users\msi2>

```

cmd Session (Right):

```

IAID DHCPv6 . . . . . : 170444242
DUID de cliente DHCPv6 . . . . . : 00-01-00-01-2E-AC-FD-77-D8-43
-AE-31-31-D4
Servidores DNS . . . . . :
    10.0.0.1
    fe80::1%18
NetBIOS sobre TCP/IP. . . . . : habilitado

Adaptador de Ethernet Conexión de red Bluetooth:
Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . . . . :
Descripción . . . . . : Bluetooth Device (Personal Area Network)
Dirección física. . . . . : 28-C5-D2-02-F2-D7
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . . . : sí

Adaptador de Ethernet Ethernet 2:
Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . . . . :
Descripción . . . . . : Realtek PCIe GbE Family Controller #2
Dirección física. . . . . : D8-43-AE-31-31-D4
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . . . : sí

C:\Users\msi2> ping 8.8.8.8

Haciendo ping a 8.8.8.8 con 32 bytes de datos:
Respueta desde 8.8.8.8: bytes=32 tiempo=37ms TTL=118
Respueta desde 8.8.8.8: bytes=32 tiempo=36ms TTL=118
Respueta desde 8.8.8.8: bytes=32 tiempo=39ms TTL=118
Respueta desde 8.8.8.8: bytes=32 tiempo=37ms TTL=118

Estadísticas de ping para 8.8.8.8:
Paquetes: enviados = 4, recibidos = 4, perdidos = 0
(0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 36ms, Máximo = 39ms, Media = 37ms
C:\Users\msi2>

```

¿Cuáles son los resultados?

ipconfig /all: verás adaptadores de red, direcciones IPv4/IPv6, máscara y gateway.

ping 8.8.8.8: recibirás paquetes de respuesta (latencia) o tiempo de espera si no hay conectividad.

cd te enseña la ruta pwd igual

Parte 3: Estudien cmdlets.

- Los comandos de PowerShell, cmdlets, se construyen como una cadena de *verbo-sustantivo*. Para identificar el comando de PowerShell que se utilizará para generar una lista de los subdirectorios y archivos presentes en un directorio, introduzcan **Get-Alias dir** en el cursor de PowerShell.

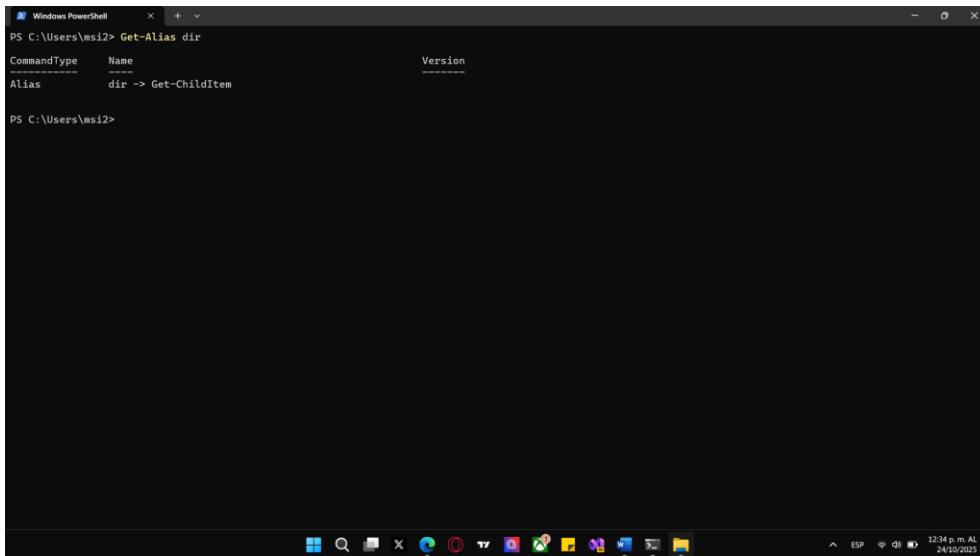
Práctica de laboratorio: Utilizar Windows PowerShell

```
PS C:\Users\CyberOpsUser> Get-Alias dir
```

```
 CommandType Name Version Source
```

```
-----  
 Aliasdir -> Get-ChildItem
```

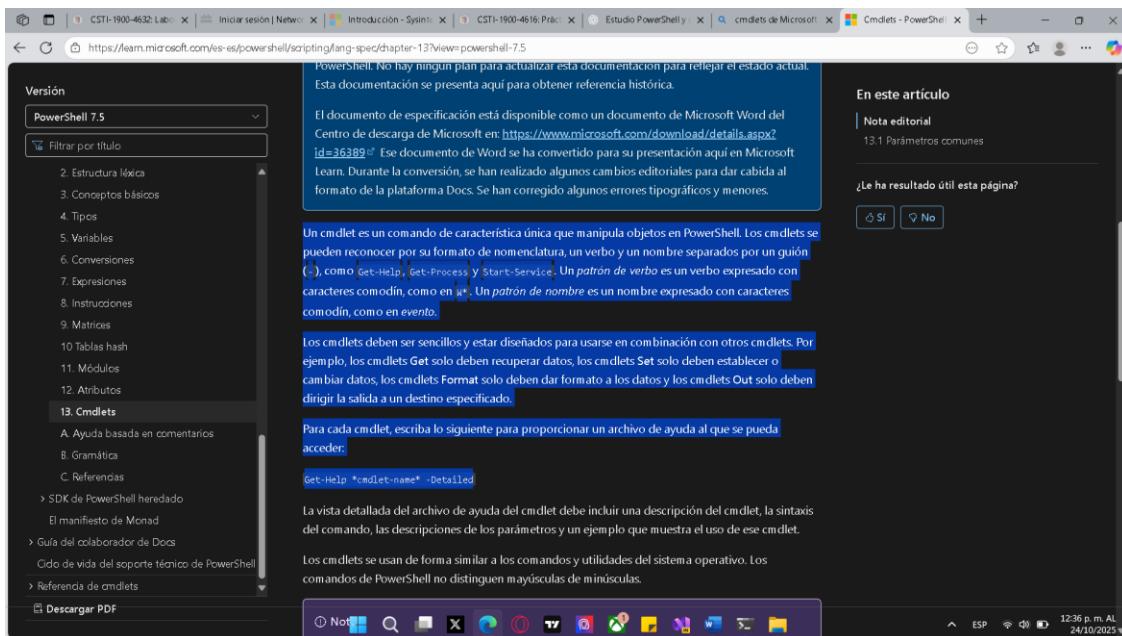
¿Cuál es el comando de PowerShell correspondiente a **dir**?



```
Windows PowerShell  
PS C:\Users\msi2> Get-Alias dir  
 CommandType Name Version Source  
-----  
 Aliasdir -> Get-ChildItem  
  
PS C:\Users\msi2>
```

El comando de PowerShell correspondiente a **dir** es **Get-ChildItem**.

- c. Para obtener información más detallada acerca de los cmdlets, realice una búsqueda en Internet de los **cmdlets de Microsoft PowerShell**.



Versión
PowerShell 7.5
Filtrar por título

2. Estructura lógica
3. Conceptos básicos
4. Tipos
5. Variables
6. Conversiones
7. Expresiones
8. Instrucciones
9. Matrices
10. Tablas hash
11. Módulos
12. Atributos
13. Cmdlets

A. Ayuda basada en comentarios
B. Gramática
C. Referencias

> SDK de PowerShell heredado
El manifiesto de Monad
> Guía del colaborador de Docs
Código de vida del soporte técnico de PowerShell
> Referencia de cmdlets

Descargar PDF

PowerShell. No hay ningún plan para actualizar esta documentación para reflejar el estado actual. Esta documentación se presenta aquí para obtener referencia histórica.

Este documento de especificación está disponible como un documento de Microsoft Word del Centro de descarga de Microsoft en <https://www.microsoft.com/download/details.aspx?id=36389>. Este documento de Word se ha convertido para su presentación aquí en Microsoft Learn. Durante la conversión, se han realizado algunos cambios editoriales para dar cabida al formato de la plataforma Docs. Se han corregido algunos errores tipográficos y menores.

Un cmdlet es un comando de característica única que manipula objetos en PowerShell. Los cmdlets se pueden reconocer por su formato de nomenclatura, un verbo y un nombre separados por un guion (-), como `Get-Help`, `Get-Process` y `Start-Service`. Un *patrón de verbo* es un verbo expresado con caracteres comodín, como en `*-*`. Un *patrón de nombre* es un nombre expresado con caracteres comodín, como en `event*`.

Los cmdlets deben ser sencillos y estar diseñados para usarse en combinación con otros cmdlets. Por ejemplo, los cmdlets `Get` solo deben recuperar datos, los cmdlets `Set` solo deben establecer o cambiar datos, los cmdlets `Format` solo deben dar formato a los datos y los cmdlets `Out` solo deben dirigir la salida a un destino especificado.

Para cada cmdlet, escriba lo siguiente para proporcionar un archivo de ayuda al que se pueda acceder:

`Get-Help *cmdlet-name* -Detailed`

La vista detallada del archivo de ayuda del cmdlet debe incluir una descripción del cmdlet, la sintaxis del comando, las descripciones de los parámetros y un ejemplo que muestra el uso de ese cmdlet.

Los cmdlets se usan de forma similar a los comandos y utilidades del sistema operativo. Los comandos de PowerShell no distinguen mayúsculas de minúsculas.

- c. Cierren la ventana del símbolo del sistema cuando hayan terminado.

Parte 4: Estudien el comando netstat utilizando PowerShell.

- a. En el PowerShell, introduzca **netstat -h** para ver las opciones disponibles para el comando **netstat**

```
PS C:\Users\CyberOpsUser> netstat -h
```

Displays protocol statistics and current TCP/IP network connections.

NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-x] [-t] [interval]

-a Displays all connections and listening ports.

-b Displays the executable involved in creating each connection or listening port. In some cases well-known executables host multiple independent components, and in these cases the sequence of components involved in creating the connection or listening port is displayed. In this case the executable name is in [] at the bottom, on top is the component it called, and so forth until TCP/IP was reached. Note that this option can be time-consuming and will fail unless you have sufficient permissions.

<some output omitted>

Socket Handle Count		
PID	Count	Closing Count
4024	20	0
8280	35	0
6416	1	0
792	2	0
2322	0	0
6988	2	0
1844	14	1
16292	7	0
140	4	0
13124	1	0
9288	1	0
9880	166	0
6788	1	0
1380	0	0
3672	1	0
17248	1	0
2484	1	0
7220	1	0
15216	3	0
7828	12	0
6788	1	0
3240	0	0
18852	31	0
6548	4	0
3992	4	0
7604	2	0
16284	2	0
2216	5	0
6828	1	0
2228	0	1
3704	4	1
5816	4	0
7368	3	0
16836	2	0
1740	111	0
6872	8	0
6628	6	0
6628	4	1
15888	3	0

Me salió los stock handles count

- b. Para mostrar la tabla de routing con las rutas activas, introduzcan **netstat -r** en el cursor.

```
PS C:\Users\CyberOpsUser> netstat -r
```

=====

Interface List

```
3...08 00 27 a0 c3 53 .....Intel(R) PRO/1000 MT Desktop Adapter
10...08 00 27 26 c1 78 .....Intel(R) PRO/1000 MT Desktop Adapter #2
1.....Software Loopback Interface 1
=====
```

IPv4 Route Table

Active Routes:

Network	Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	192.168.1.1	192.168.1.5	25	
127.0.0.0	255.0.0.0	On-link	127.0.0.1	331	
127.0.0.1	255.255.255.255	On-link	127.0.0.1	331	
127.255.255.255	255.255.255.255	On-link	127.0.0.1	331	
169.254.0.0	255.255.0.0	On-link	169.254.181.151	281	
169.254.181.151	255.255.255.255	On-link	169.254.181.151	281	
169.254.255.255	255.255.255.255	On-link	169.254.181.151	281	
192.168.1.0	255.255.255.0	On-link	192.168.1.5	281	

```
192.168.1.5 255.255.255.255 On-link 192.168.1.5 281
192.168.1.255 255.255.255.255 On-link 192.168.1.5 281
224.0.0.0 240.0.0.0 On-link 127.0.0.1 331
224.0.0.0 240.0.0.0 On-link 192.168.1.5 281
224.0.0.0 240.0.0.0 On-link 169.254.181.151 281
255.255.255.255 255.255.255.255 On-link 127.0.0.1 331
255.255.255.255 255.255.255.255 On-link 192.168.1.5 281
255.255.255.255 255.255.255.255 On-link 169.254.181.151 281
```

Persistent Routes:

None

IPv6 Route Table

Active Routes:

If Metric Network Destination Gateway

1 331 ::1/128 On-link

3 281 fe80::/64 On-link

10 281 fe80::/64 On-link

10 281

On-link

3 281 f

On-link

1 331 ff00::/8 On-link

3 281 ff00::/8 On-link

```
10 281 ff00::/8 On-link  
=====  
Persistent Routes:
```

Persistent Routes:

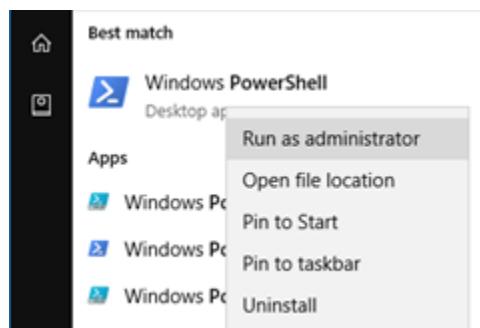
None

¿Qué es el gateway IPv4?

Gateway IPv4: 192.168.0.1

Es la dirección IP de la puerta de enlace predeterminada, que actúa como el punto de conexión entre la red local del equipo y otras redes (como Internet).

- c. Abran y ejecuten una segunda PowerShell con privilegios elevados. Hagan clic en **Inicio**. Busquen PowerShell, hagan clic derecho en **Windows PowerShell** y seleccione **Run as Administrator** (Ejecutar como administrador). Hagan clic en **Yes** (Sí) para permitir que esta aplicación realice cambios en sus dispositivos.



- d. El comando netstat también puede mostrar los procesos asociados con las conexiones TCP activas. Introduzcan el comando **netstat -abno** en el cursor.

```
PS C:\Windows\system32> netstat -abno
```

```
Active Connections

Proto Local Address Foreign Address State PID
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING 756
RpcSs
[svchost.exe]
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING 4
Can not obtain ownership information
TCP 0.0.0.0:49664 0.0.0.0:0 LISTENING 444
Can not obtain ownership information
TCP 0.0.0.0:49665 0.0.0.0:0 LISTENING 440
Schedule
[svchost.exe]
TCP 0.0.0.0:49666 0.0.0.0:0 LISTENING 304
EventLog
[svchost.exe]
TCP 0.0.0.0:49667 0.0.0.0:0 LISTENING 1856
[spoolsv.exe]
TCP 0.0.0.0:49668 0.0.0.0:0 LISTENING 544
<some output omitted>
```

Práctica de laboratorio: Utilizar Windows PowerShell

```
Administrator: Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

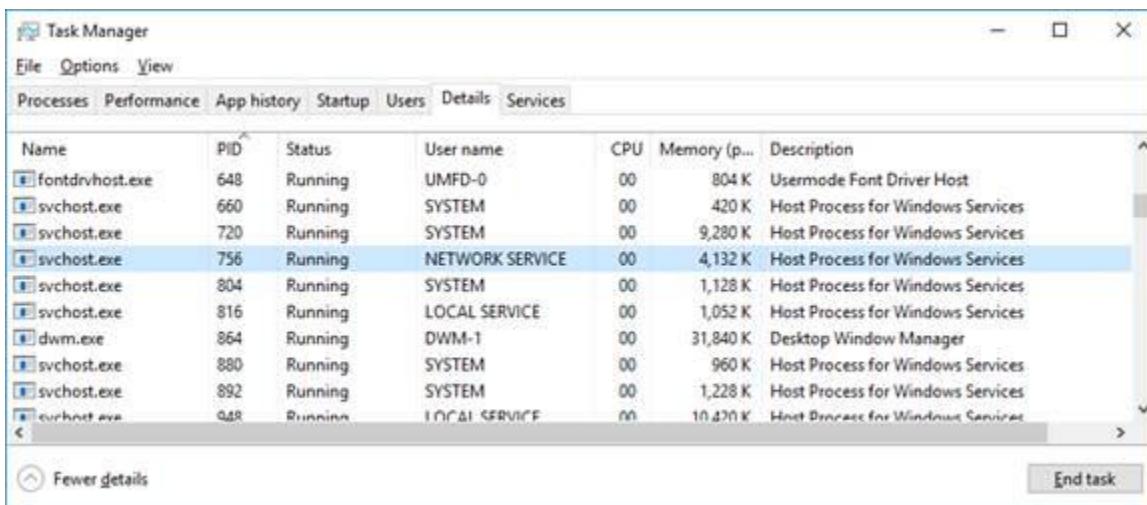
Instale la versión más reciente de PowerShell para obtener nuevas características y mejoras. https://aka.ms/PSWindows

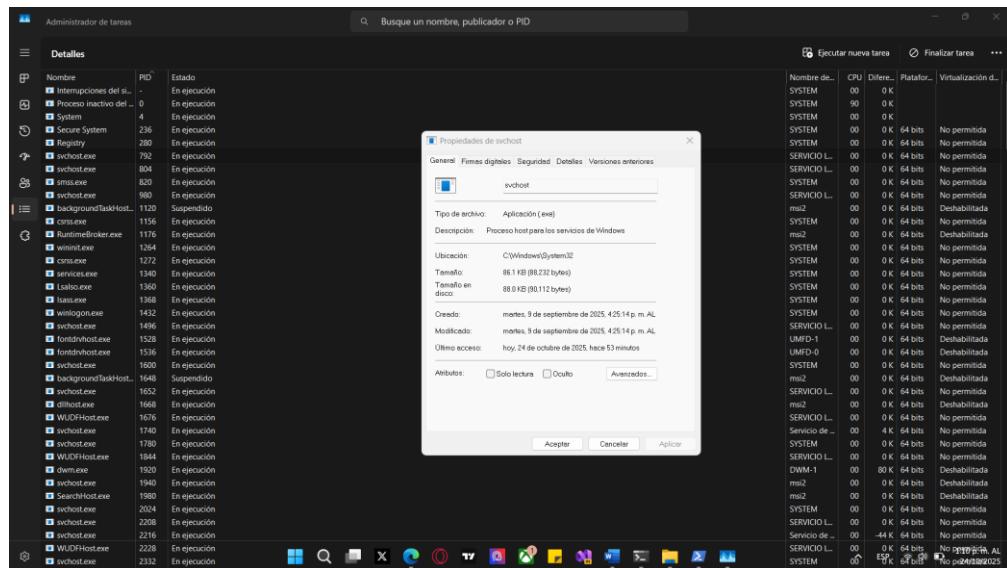
PS C:\Windows\system32> netstat -abno

Conexiones activas

Proto Dirección local     Dirección remota   Estado      PID
TCP  0.0.0.0.135          0.0.0.0.0       LISTENING  1740
[wpqhttpd.exe]
[TCP...0.0.0.0.465
No se puede obtener información de propiedades
TCP  0.0.0.0.1392         0.0.0.0.0       LISTENING  7144
[win32kfull.exe]
TCP  0.0.0.0.1912         0.0.0.0.0       LISTENING  7144
[win32kfull.exe]
TCP  0.0.0.0.1912         0.0.0.0.0       LISTENING  7144
[win32kfull.exe]
No se puede obtener información de propiedades
TCP  0.0.0.0.1940         0.0.0.0.0       LISTENING  4
[win32kfull.exe]
No se puede obtener información de propiedades
TCP  0.0.0.0.1940         0.0.0.0.0       LISTENING  10292
CDPSvc
[wpqhost.exe]
TCP  0.0.0.0.5357         0.0.0.0.0       LISTENING  4
No se puede obtener información de propiedades
TCP  0.0.0.0.14964        0.0.0.0.0       LISTENING  1368
No se puede obtener información de propiedades
TCP  0.0.0.0.49955        0.0.0.0.0       LISTENING  1284
No se puede obtener información de propiedades
TCP  0.0.0.0.14966        0.0.0.0.0       LISTENING  2332
[wpqhost.exe]
TCP  0.0.0.0.14967        0.0.0.0.0       LISTENING  3992
EventLog
[wpqhost.exe]
TCP  0.0.0.0.14968        0.0.0.0.0       LISTENING  5816
[spoolsv.exe]
TCP  0.0.0.0.14970        0.0.0.0.0       LISTENING  1340
No se puede obtener información de propiedades
TCP  10.0.0.37-139         0.0.0.0.0       LISTENING  4
No se puede obtener información de propiedades
TCP  10.0.0.37-11893       66.98.4.25-86    TIME_WAIT  0
TCP  10.0.0.37-20524       135.234.174.40-463  ESTABLISHED 10852
[msedge.exe]
TCP  10.0.0.37-52291       20.189.173.12-443  FIN_WAIT_1 10852
[msedge.exe]
TCP  10.0.0.37-8529        127.0.0.1-65001  ESTABLISHED 7028
[rvicontainer.exe]
TCP  127.0.0.1-18541       0.0.0.0.0       LISTENING  8200
[NVIDIA Web Helper.exe]
TCP  127.0.0.1-18541       127.0.0.1-50823  ESTABLISHED 1040
```

- e. Abran el Administrador de tareas. Diríjanse a la ficha **Details** (Detalles). Hagan clic en el encabezado **PID** para que los PID estén en orden.
- f. Selecionen uno de los PID de los resultados de netstat -abno. En este ejemplo se utiliza el PID 756.
- g. Localicen el PID seleccionado en el Administrador de tareas. En el Administrador de tareas, hagan clic derecho sobre el PID seleccionado para abrir el cuadro de diálogo **Properties** (Propiedades) y ver más información.





¿Qué información pueden obtener de la ficha Details y del cuadro de diálogo Properties correspondientes al PID que seleccionaron?

En la ficha *Details* se ve el nombre, estado y PID del proceso.

En *Properties* se muestra la ruta, descripción y firma digital del archivo.

Esta información permite saber si el proceso es del sistema o potencialmente sospechoso.

Parte 5: Vaciar la papelera de reciclaje utilizando PowerShell.

Los comandos de PowerShell pueden simplificar la administración de una gran de red informática. Por ejemplo: si quieren implementar una nueva solución de seguridad en todos los servidores de la red, podrían utilizar un comando o script de PowerShell para implementar los servicios y verificar que estén funcionando. También pueden ejecutar comandos de PowerShell para simplificar acciones cuya ejecución requeriría varios pasos de utilizar las herramientas de escritorio gráficas de Windows.

- Abran la Papelera de reciclaje. Verifiquen que haya elementos que se puedan eliminar de su PC en forma permanente. Si no es así, restauren esos archivos.
- Si no hay ningún archivo en la Papelera de reciclaje, creen uno nuevo (como ser un archivo de texto con el Bloc de notas) y colóquenlo en la Papelera.
- En una consola de PowerShell introduzcan **clear-recyclebin** en el cursor.

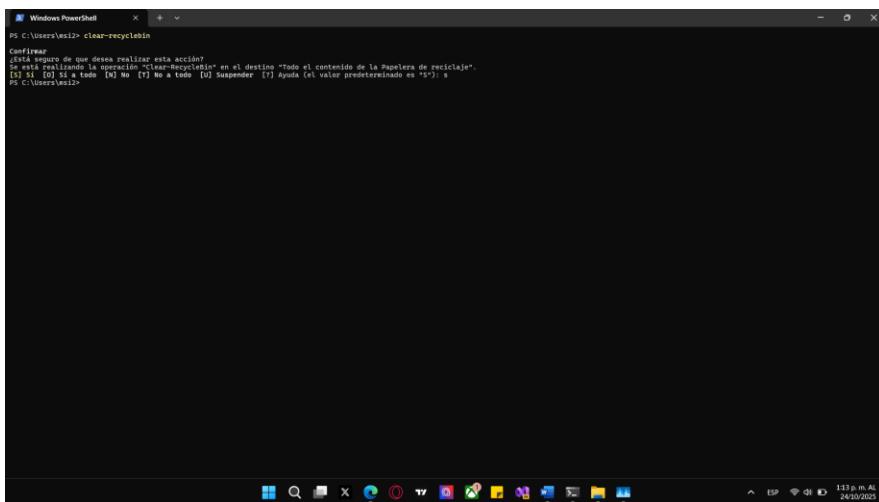
```
PS C:\Users\CyberOpsUser> clear-recyclebin
```

Confirm

Are you sure you want to perform this action?

Performing the operation "Clear-RecycleBin" on target "All of the contents of the Recycle Bin".

```
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): y
```



¿Qué sucedió con los archivos de la Papelera de reciclaje?

Todos los archivos almacenados en la Papelera de reciclaje fueron eliminados de manera permanente del sistema. Después de ejecutar el comando Clear-RecycleBin, la Papelera quedó vacía y los elementos ya no pueden recuperarse desde la interfaz gráfica.

Pregunta de reflexión

PowerShell fue desarrollado para la automatización de tareas y la administración de la configuración. Utilizando el internet, realice una búsqueda de comandos que pueden simplificar sus tareas como analista de seguridad. Registren sus conclusiones.

PowerShell incluye una amplia variedad de comandos que pueden ayudar en las tareas de un analista de seguridad. Algunos ejemplos son:

- Get-EventLog → Permite revisar y filtrar registros de eventos del sistema para detectar actividad sospechosa.
- Get-Process y Stop-Process → Muestran o detienen procesos sospechosos activos en el sistema.
- Get-Service → Verifica el estado de servicios importantes y detecta servicios desconocidos o maliciosos.
- Test-Connection → Comprueba la conectividad con otros equipos de la red (similar al comando *ping*).
- Get-NetTCPConnection → Lista las conexiones TCP actuales, útil para identificar puertos abiertos o conexiones inusuales.
- Set-ExecutionPolicy → Controla las políticas de ejecución de scripts, fortaleciendo la seguridad del sistema.

Estos comandos ayudan a automatizar auditorías, monitorear actividad de red y mantener una configuración segura en entornos corporativos.