Práctica de laboratorio: Utilizar Windows PowerShell

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

b. Prueben otro comando que hayan utilizando en el símbolo del sistema, como **ping**, **cd** o **ipconfig**.
¿Cuáles son los resultados?

Parte 3: Estudien cmdlets.

a. 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.

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

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

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

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

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

Muestra estadísticas de protocolos y las conexiones de red TCP/IP actuales.

NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-x] [-t] [interval]
 -a Displays all connections and listening ports.
  -b muestra el ejecutable que se utiliza para crear cada puerto de conexión o
escucha. En algunos casos, los ejecutables más conocidos alojan varios componentes
independientes, y en estos casos se muestra la secuencia de componentes que se utiliza
para crear el puerto de conexión o escucha. En este caso, el nombre del archivo
ejecutable se encuentra entre los signos [] en la parte inferior, arriba se encuentra
el componente al que le da nombre, y así sucesivamente hasta que se alcanza TCP/IP.
Tenga en cuenta que esta opción demanda tiempo y fallará a menos que cuente con los
permisos suficientes.
<some output omitted>
```

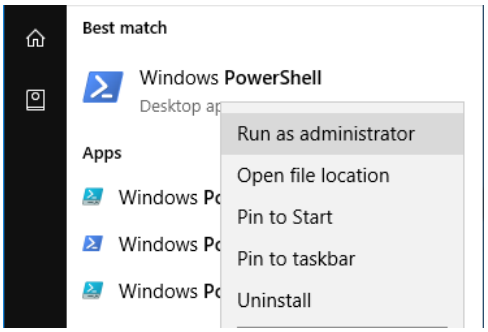
b. Para mostrar la tabla de routing con las rutas activas, introduzcan **netstat -r** en el cursor.

```
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

Tabla de routing IPv6
===========================================================================
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 fe80::408b:14a4:7b64:b597/128
                                    On-link
  3 281 fe80::dd67:9e98:9ce0:51e/128
                                    On-link
  1 331 ff00::/8 On-link
  3 281 ff00::/8 On-link
 10 281 ff00::/8 On-link
===========================================================================
Persistent Routes:
  None
```

¿Qué es el gateway IPv4?

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.



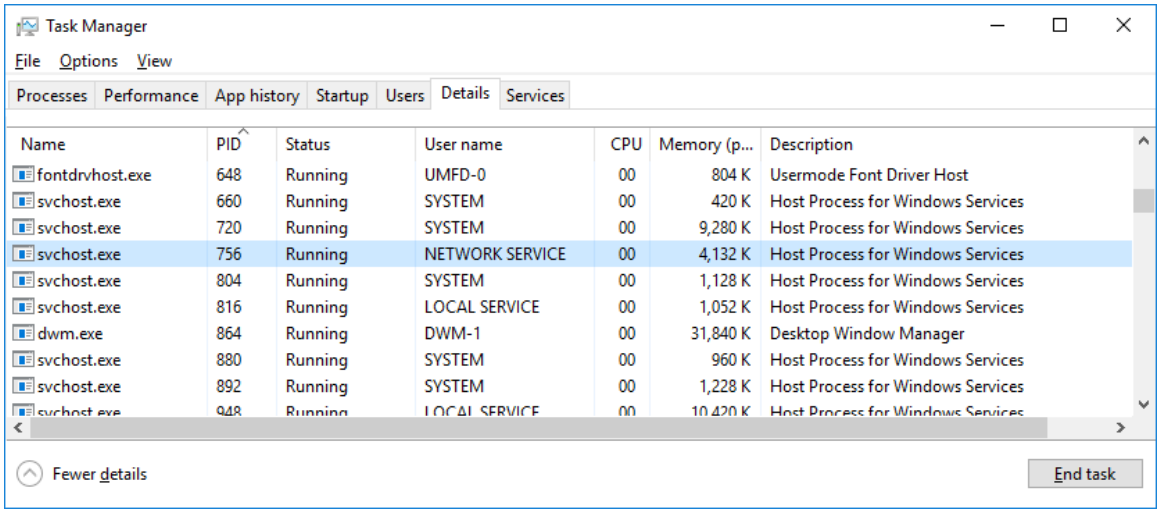
d. El comando netstat también puede mostrar los procesos asociados con las conexiones TCP activas. Introduzca el comando **netstat -abno** en el indicador.

```
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>
```

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. Seleccionen 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?

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.

a. 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.

b. Si no hay ningún archivo en la Papelera de reciclaje, creen uno nuevo (como puede ser un archivo de texto con el Bloc de notas) y colóquenlo en la Papelera.

c. 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?

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.