Laboratório - Usando o Windows PowerShell

# Objetivos

O objetivo do laboratório é explorar algumas das funções do PowerShell.

Parte 1: Acesse o console do PowerShell.

Parte 2: Explore comandos do Prompt de Comando e do PowerShell.

Parte 3: Explore cmdlets.

Parte 4: Explore o comando netstat usando o PowerShell.

Parte 5: Esvazie a lixeira usando o PowerShell.

# Histórico/Cenário

O PowerShell é uma poderosa ferramenta de automação. É um console de comando e uma linguagem de script. Neste laboratório, você usará o console para executar alguns dos comandos disponíveis no prompt de comando e no PowerShell. O PowerShell também possui funções que podem criar scripts para automatizar tarefas e trabalhar em conjunto com o Sistema Operacional Windows.

# Recursos necessários

=   1 PC Windows com PowerShell instalado e acesso à Internet

# Instruções

## Parte 1: Acesse o console do PowerShell.

a.     Clique em **Iniciar**. Pesquise e selecione **powershell**.

b.     Clique em **Iniciar**. Pesquise e selecione o **prompt de comando**.

## Parte 2: Explore comandos do Prompt de Comando e do PowerShell.

a.     Digite **dir** no prompt em ambas as janelas.

### Pergunta:

Quais são as saídas para o comando **dir**?

***Área de Resposta***

b.     Tente outro comando que você usou no prompt de comando, como **ping**, **cd** e **ipconfig**.

### Pergunta:

Quais são os resultados?

***Área de Resposta***

## Parte 3: Explore cmdlets.

a.     Comandos do PowerShell, cmdlets, são construídos na forma de *verb-noun* string Para identificar o comando do PowerShell para listar os subdiretórios e arquivos em um diretório, digite **Get-Alias dir** no prompt do PowerShell.

PS C:\Users\CyberOpsUser > **Dir de Get-Alias**

CommandTypenaVersionSource

----------------------------

Aliasdir -> Get-ChildItem

### Pergunta:

O que é o comando do PowerShell para **dir**?

***Área de Resposta***

b.     Para obter informações mais detalhadas sobre cmdlets, execute uma pesquisa na Internet para **cmdlets do Microsoft Powershell**.

c.     Feche a janela do prompt de comando quando terminar.

## Parte 4: Explore o comando netstat usando o PowerShell.

a.     No prompt do PowerShell, digite **netstat -h** para ver as opções disponíveis para o comando **netstat**.

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

Exibe estatísticas de protocolo e conexões de rede TCP / IP atuais.

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

 -a Exibe todas as conexões e portas de escuta.

 -b Exibe o executável envolvido na criação de cada conexão ou porta de escuta. Em alguns casos, executáveis conhecidos hospedam vários componentes independentes e, nesses casos, a seqüência de componentes envolvidos na criação da porta de conexão ou escuta é exibida. Nesse caso, o nome do executável está entre [] na parte inferior, na parte superior está o componente que ele chamou e assim por diante até que o TCP / IP seja alcançado. Observe que essa opção pode ser demorada e falhará, a menos que você tenha permissões suficientes.

<some output omitted>

b.     Para exibir a tabela de roteamento com as rotas ativas, digite **netstat -r** no prompt.

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

=======================================================================================

Lista de Interface

 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

=======================================================================================

Rotas ativas:

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

        127.0.0.0        255.0.0.0         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

=======================================================================================

Rotas persistentes:

  Nenhuma

Tabela de roteamento IPv6

=======================================================================================

Rotas ativas:

 Se a metrica do      Gateway para a rede de destino

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

=======================================================================================

Rotas persistentes:

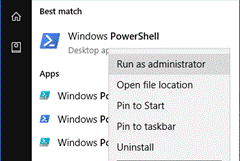
  Nenhuma

### Pergunta:

O que é o gateway IPv4?

***Área de Resposta***

c.     Abra e execute um segundo PowerShell com privilégios elevados. Clique em **Iniciar**. Procure o PowerShell e clique com o botão direito do mouse no **Windows PowerShell** e selecione **Executar como administrador**. Clique em **Sim** para permitir que este aplicativo faça alterações em seu dispositivo.



d.     O comando netstat também pode exibir os processos associados às conexões TCP ativas. Digite o **netstat -abno** no prompt.

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

Conexões ativas

 Proto  Endereço local          Endereço Estrangeiro        Estado           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

 Não é possível obter informações de propriedade

  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       444

 Não é possível obter informações de propriedade

  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       440

 Programação

 [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.     Abra o Gerenciador de Tarefas. Navegue até a guia **Detalhes** . Clique no cabeçalho **PID** para que o PID esteja em ordem.

f.      Selecione um dos PIDs dos resultados de netstat -abno. O PID 756 é usado neste exemplo.

g.     Localize o PID selecionado no Gerenciador de Tarefas. Clique com o botão direito do mouse no PID selecionado no Gerenciador de Tarefas para abrir a caixa de diálogo **Propriedades** para obter mais informações.