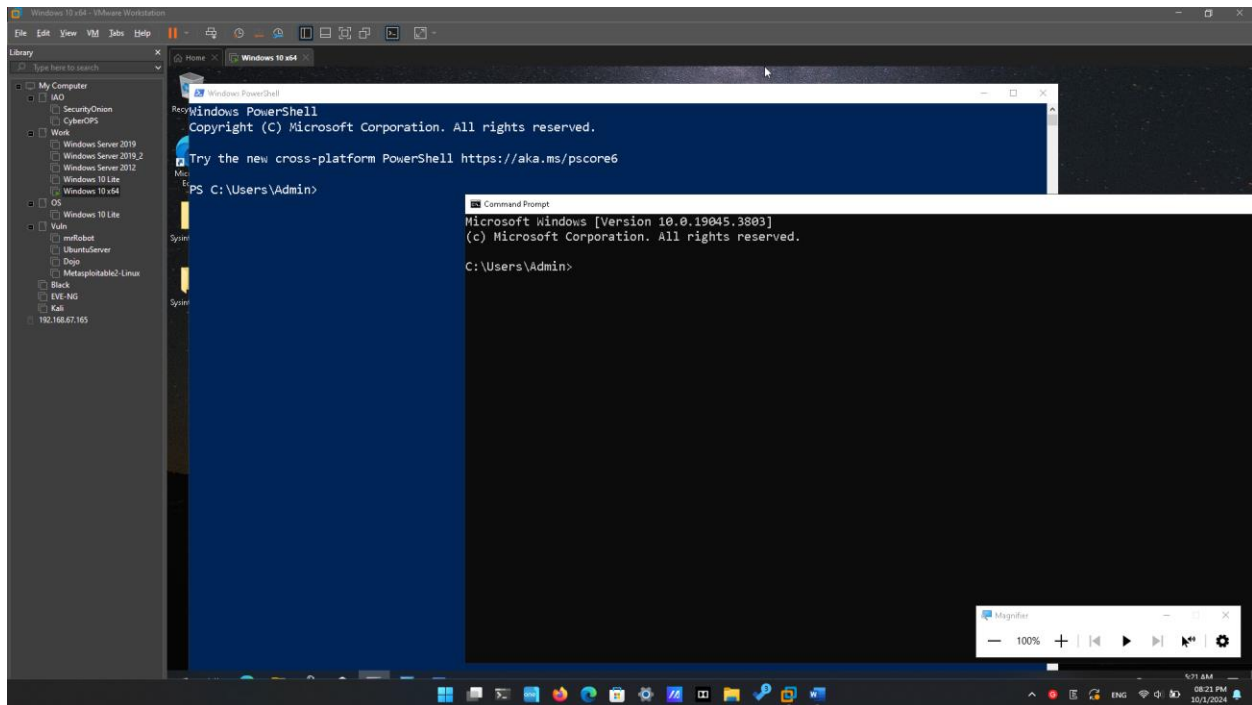


Lab - Using Windows PowerShell

Instructions

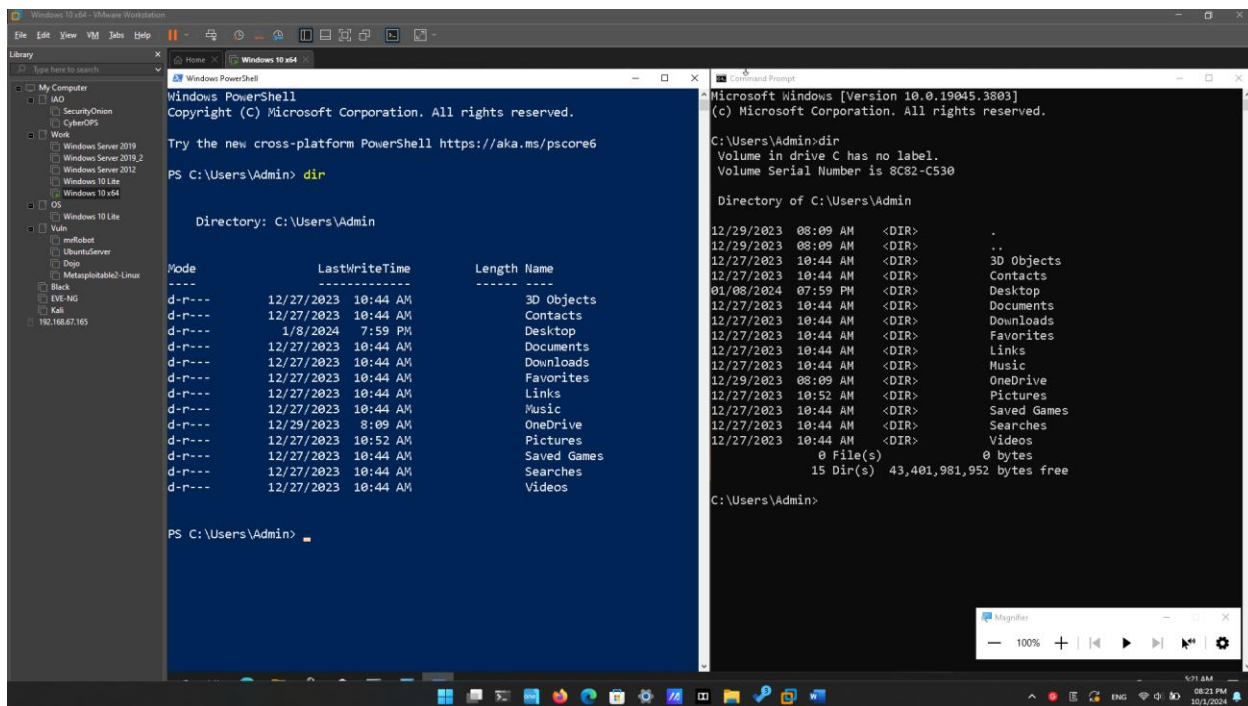
Access PowerShell console.



Explore Command Prompt and PowerShell commands.

What are the outputs to the **dir** command?

The “dir” command will show all files and folder (directories) in current folder (directory) with some additional information like Modified Time, Mode, Name, ...



Windows PowerShell

```

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\Admin> dir

Directory: C:\Users\Admin

Mode                LastWriteTime         Length Name
----                -
d-r--           12/27/2023 10:44 AM             30 Objects
d-r--           12/27/2023 10:44 AM             Contacts
d-r--           12/27/2023 10:44 AM             Desktop
d-r--           12/27/2023 10:44 AM             Documents
d-r--           12/27/2023 10:44 AM             Downloads
d-r--           12/27/2023 10:44 AM             Favorites
d-r--           12/27/2023 10:44 AM             Links
d-r--           12/27/2023 10:44 AM             Music
d-r--           12/27/2023 10:44 AM             OneDrive
d-r--           12/27/2023 10:44 AM             Pictures
d-r--           12/27/2023 10:44 AM             Saved Games
d-r--           12/27/2023 10:44 AM             Searches
d-r--           12/27/2023 10:44 AM             Videos
  
```

Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.

```

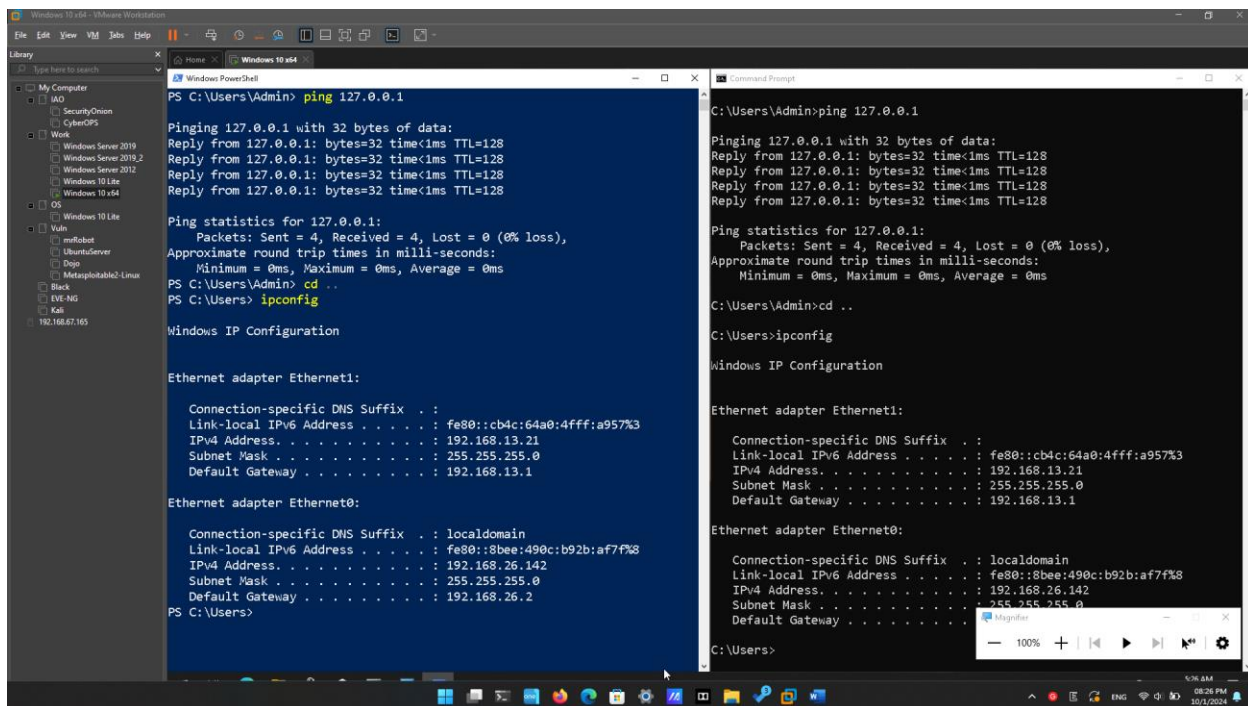
C:\Users\Admin>dir
Volume in drive C has no label.
Volume Serial Number is 8C82-C530

Directory of C:\Users\Admin

12/29/2023  08:09 AM <DIR>          .
12/29/2023  08:09 AM <DIR>          ..
12/27/2023  10:44 AM <DIR>          3D Objects
12/27/2023  10:44 AM <DIR>          Contacts
12/27/2023  10:44 AM <DIR>          Desktop
01/08/2024  07:59 PM <DIR>          Documents
12/27/2023  10:44 AM <DIR>          Downloads
12/27/2023  10:44 AM <DIR>          Favorites
12/27/2023  10:44 AM <DIR>          Links
12/27/2023  10:44 AM <DIR>          Music
12/27/2023  10:52 AM <DIR>          OneDrive
12/27/2023  10:44 AM <DIR>          Pictures
12/27/2023  10:44 AM <DIR>          Saved Games
12/27/2023  10:44 AM <DIR>          Searches
12/27/2023             0 File(s)            0 bytes
12/27/2023             15 Dir(s)      43,401,981,952 bytes free

C:\Users\Admin>
  
```

Try another command that you have used in the command prompt, such as **ping**, **cd**, and **ipconfig**. What are the results?



Windows PowerShell

```

PS C:\Users\Admin> ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

PS C:\Users\Admin> cd ..

PS C:\Users> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet1:

    Connection-specific DNS Suffix  . : fe80::cb4c:64a0:4fff:a957%3
    Link-local IPv6 Address . . . . . : fe80::cb4c:64a0:4fff:a957%3
    IPv4 Address. . . . . : 192.168.13.21
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.13.1

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : localdomain
    Link-local IPv6 Address . . . . . : fe80::8bee:490c:b92b:af7f%8
    IPv4 Address. . . . . : 192.168.26.142
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.26.2

PS C:\Users>
  
```

Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.

```

C:\Users\Admin>ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Admin>cd ..

C:\Users>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet1:

    Connection-specific DNS Suffix  . : fe80::cb4c:64a0:4fff:a957%3
    Link-local IPv6 Address . . . . . : fe80::cb4c:64a0:4fff:a957%3
    IPv4 Address. . . . . : 192.168.13.21
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.13.1

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : localdomain
    Link-local IPv6 Address . . . . . : fe80::8bee:490c:b92b:af7f%8
    IPv4 Address. . . . . : 192.168.26.142
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.26.2

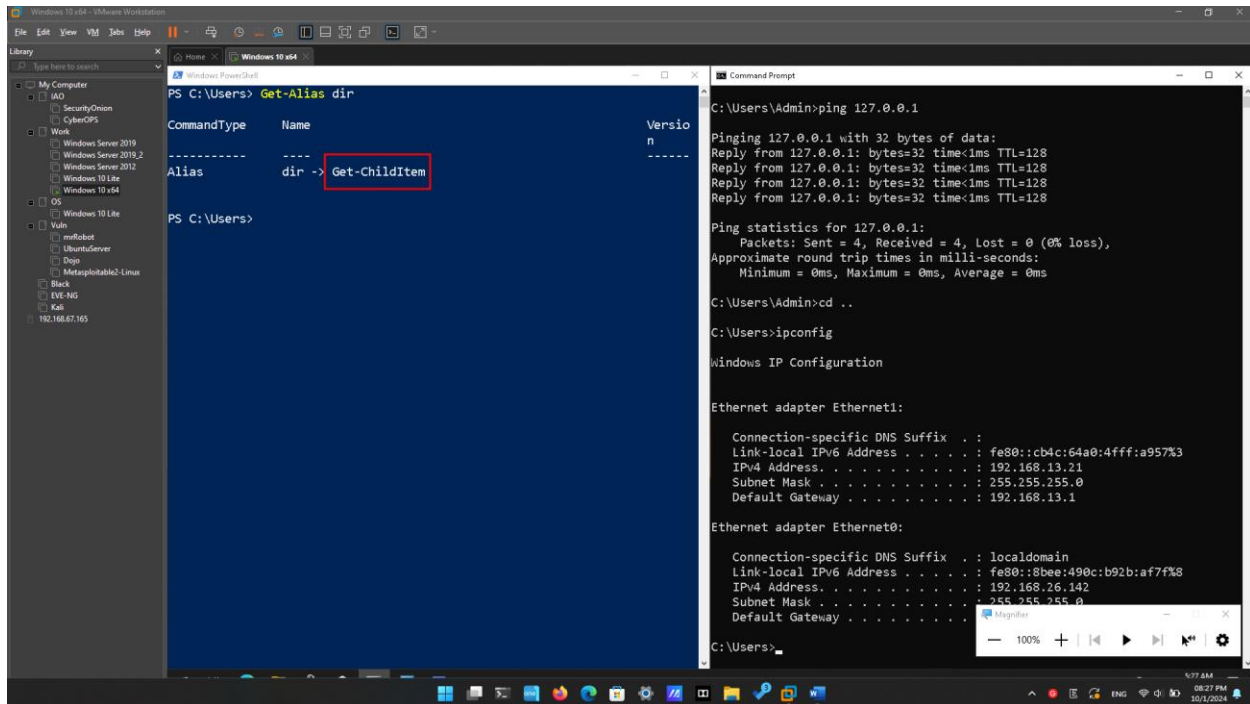
C:\Users>
  
```

They also have the same outputs.

Explore cmdlets.

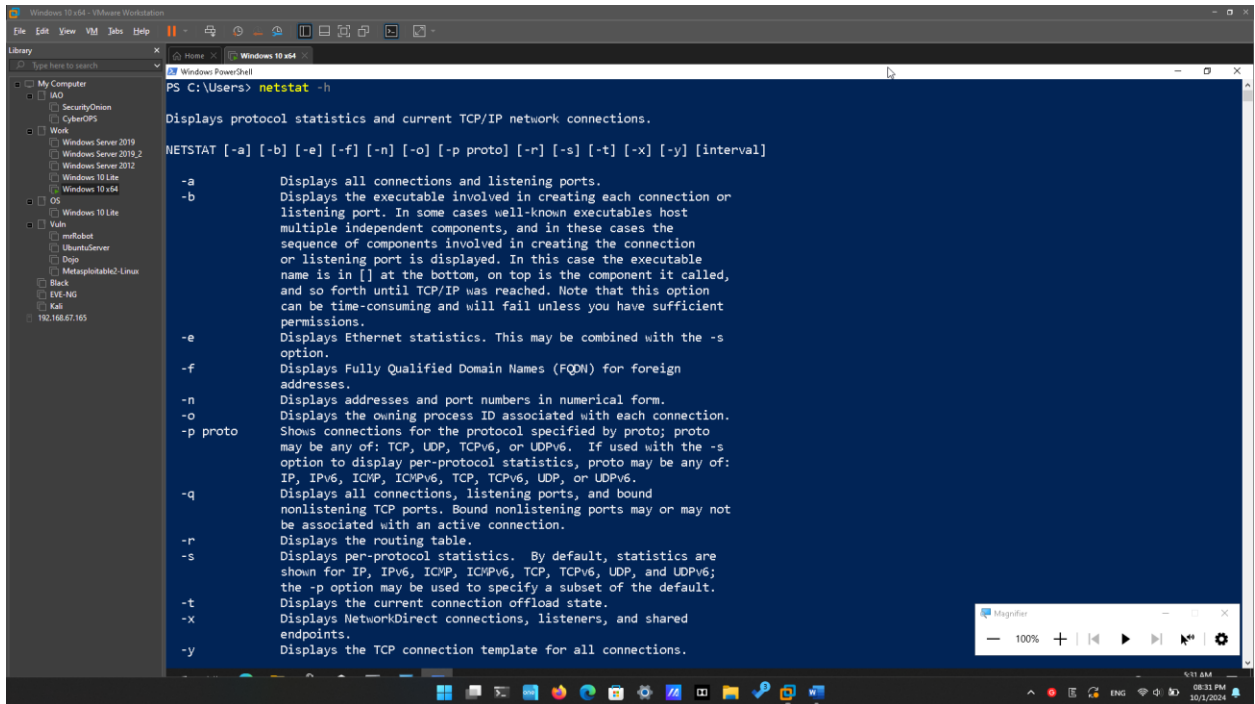
What is the PowerShell command for **dir**?

Get-ChildItem



Explore the netstat command using PowerShell.

At the PowerShell prompt, enter **netstat -h** to see the options available for the **netstat** command.



```

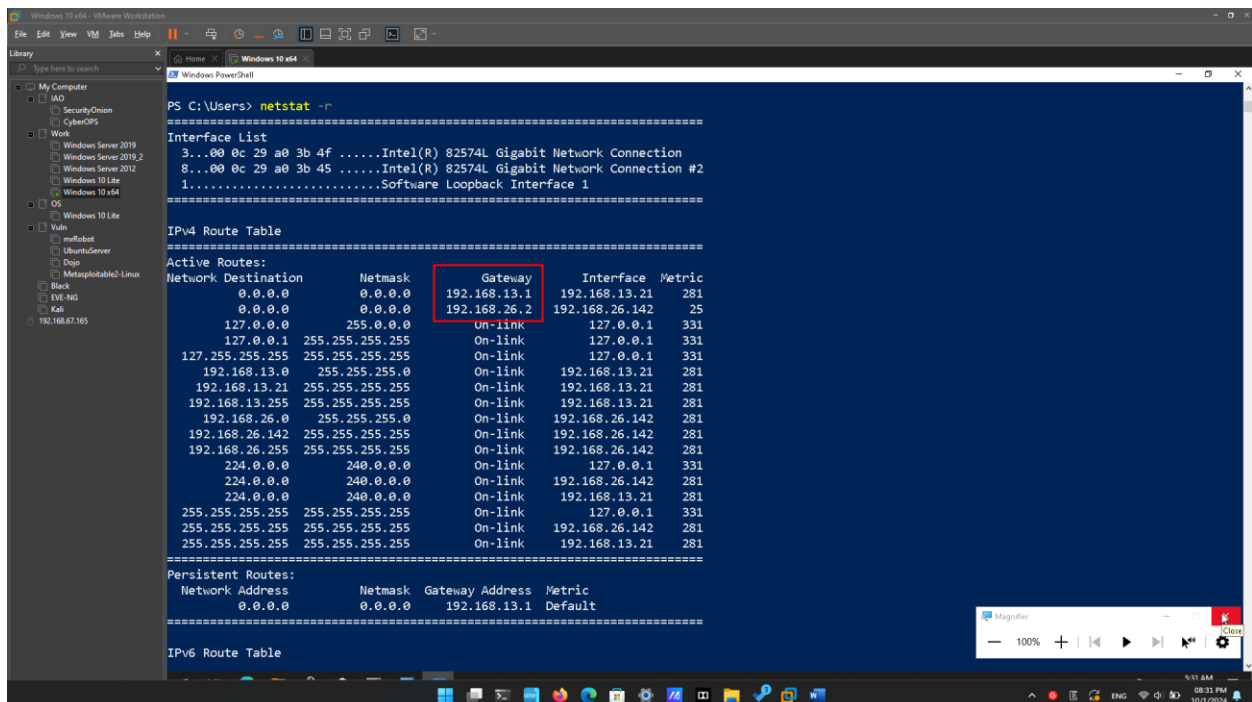
PS C:\Users> netstat -h

Displays protocol statistics and current TCP/IP network connections.

NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-t] [-x] [-y] [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.
-e          Displays Ethernet statistics. This may be combined with the -s
           option.
-f          Displays Fully Qualified Domain Names (FQDN) for foreign
           addresses.
-n          Displays addresses and port numbers in numerical form.
-o          Displays the owning process ID associated with each connection.
           Shows connections for the protocol specified by proto; proto
           may be any of: TCP, UDP, TCPv6, or UDPv6. If used with the -s
           option to display per-protocol statistics, proto may be any of:
           IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, or UDPv6.
-p proto    Displays all connections, listening ports, and bound
           nonlistening TCP ports. Bound nonlistening ports may or may not
           be associated with an active connection.
-r          Displays the routing table.
-s          Displays per-protocol statistics. By default, statistics are
           shown for IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, and UDPv6;
           the -p option may be used to specify a subset of the default.
-t          Displays the current connection offload state.
-x          Displays NetworkDirect connections, listeners, and shared
           endpoints.
-y          Displays the TCP connection template for all connections.
  
```

To display the routing table with the active routes, enter **netstat -r** at the prompt.



```

PS C:\Users> netstat -r

Interface List
3...00 0c 29 a0 3b 4f .....Intel(R) 82574L Gigabit Network Connection
8...00 0c 29 a0 3b 45 .....Intel(R) 82574L Gigabit Network Connection #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          192.168.13.1     192.168.13.21    281
0.0.0.0                0.0.0.0          192.168.26.2     192.168.26.142   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
192.168.13.0           255.255.255.0    On-link         192.168.13.21    281
192.168.13.21          255.255.255.255 On-link         192.168.13.21    281
192.168.13.255         255.255.255.255 On-link         192.168.13.21    281
192.168.26.0           255.255.255.0    On-link         192.168.26.142   281
192.168.26.142         255.255.255.255 On-link         192.168.26.142   281
192.168.26.255         255.255.255.255 On-link         192.168.26.142   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         192.168.26.142   281
224.0.0.0              240.0.0.0        On-link         192.168.13.21    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         192.168.26.142   281
255.255.255.255        255.255.255.255 On-link         192.168.13.21    281

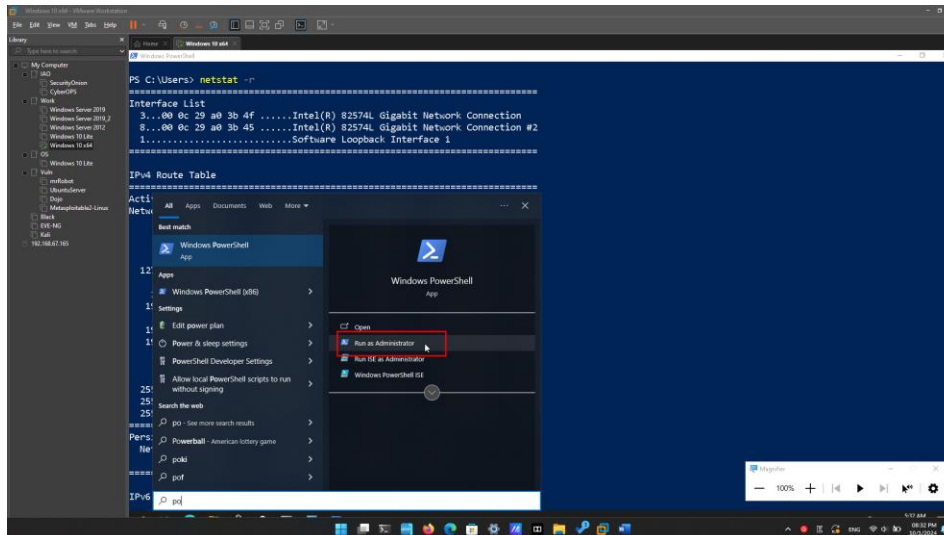
Persistent Routes:
Network Address    Netmask  Gateway Address  Metric
0.0.0.0           0.0.0.0  192.168.13.1     Default

IPv6 Route Table
=====
  
```

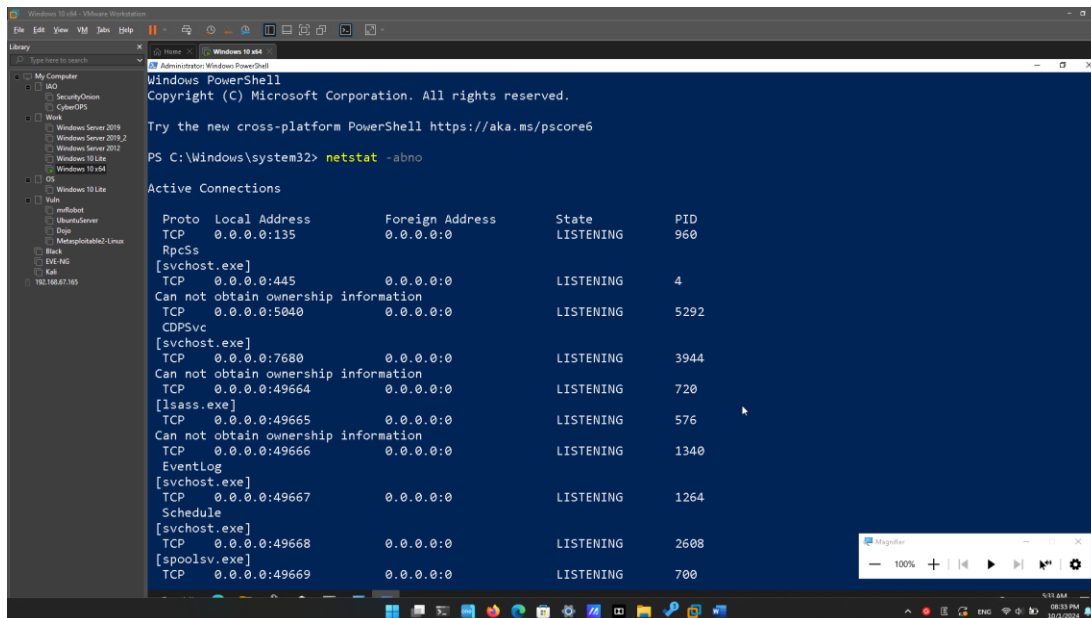
What is the IPv4 gateway?

192.168.13.1 and 192.168.26.2

Open and run a second PowerShell with elevated privileges. Click **Start**. Search for PowerShell and right-click **Windows PowerShell** and select **Run as administrator**. Click **Yes** to allow this app to make changes to your device.

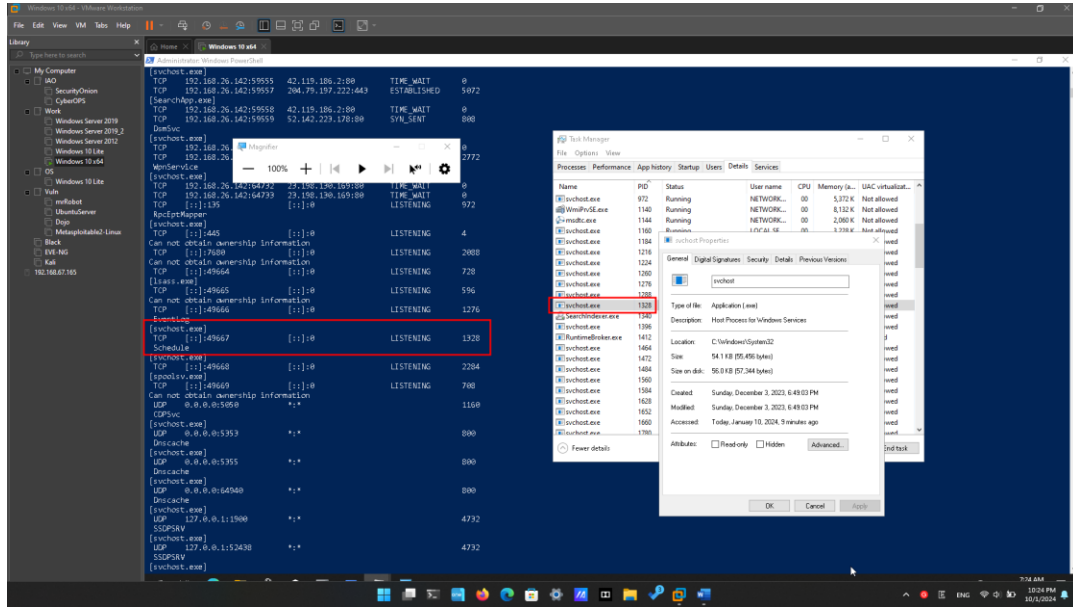


The `netstat` command can also display the processes associated with the active TCP connections. Enter the `netstat -abno` at the prompt.



Open the Task Manager. Navigate to the **Details** tab. Click the **PID** heading so the PID are in order.

What information can you get from the Details tab and the Properties dialog box for your selected PID?



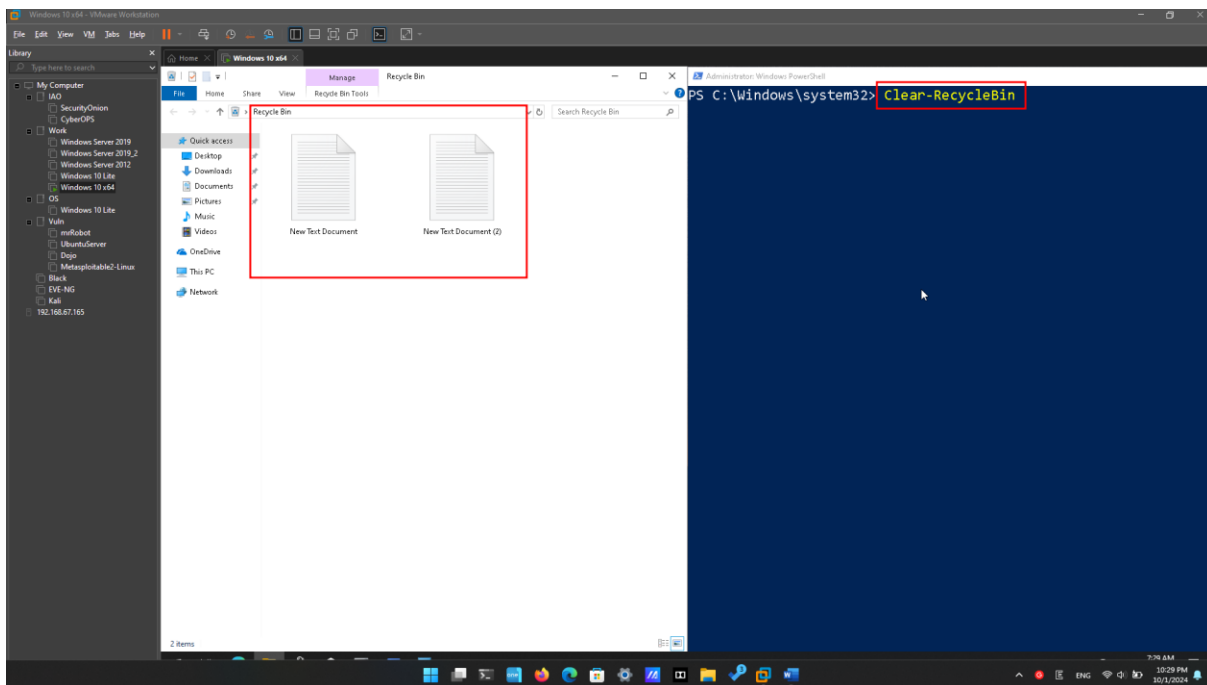
General, Digital Signature, Security, Details, Previous Version

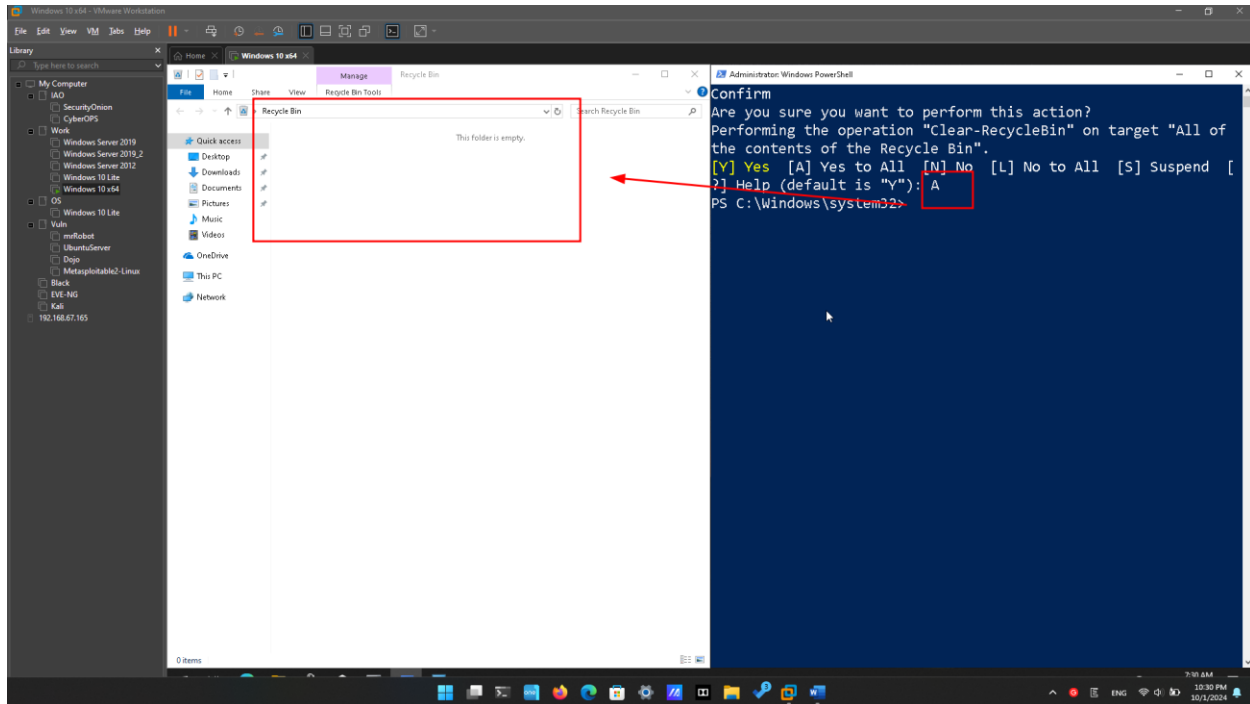
Empty recycle bin using PowerShell.

Open the Recycle Bin. Verify that there are items that can be deleted permanently from your PC. If not, restore those files.

If there are no files in the Recycle Bin, create a few files, such as text file using Notepad, and place them into the Recycle Bin.

In a PowerShell console, enter **clear-recyclebin** at the prompt





What happened to the files in the Recycle Bin?

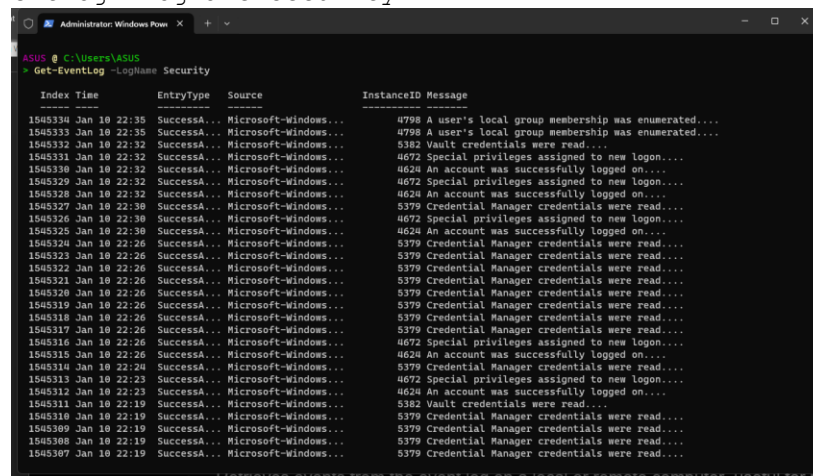
The files in the Recycle Bin are deleted.

Reflection Question

PowerShell was developed for task automation and configuration management. Using the internet, research commands that you could use to simplify your tasks as a security analyst. Record your findings.

- Retrieves events from the event log on a local or remote computer, useful for reviewing system logs for security-related events.

Get-EventLog -LogName Security



Get-NetFirewallRule:

Lists firewall rules, helping you inspect and manage the firewall configuration for enhanced security.

