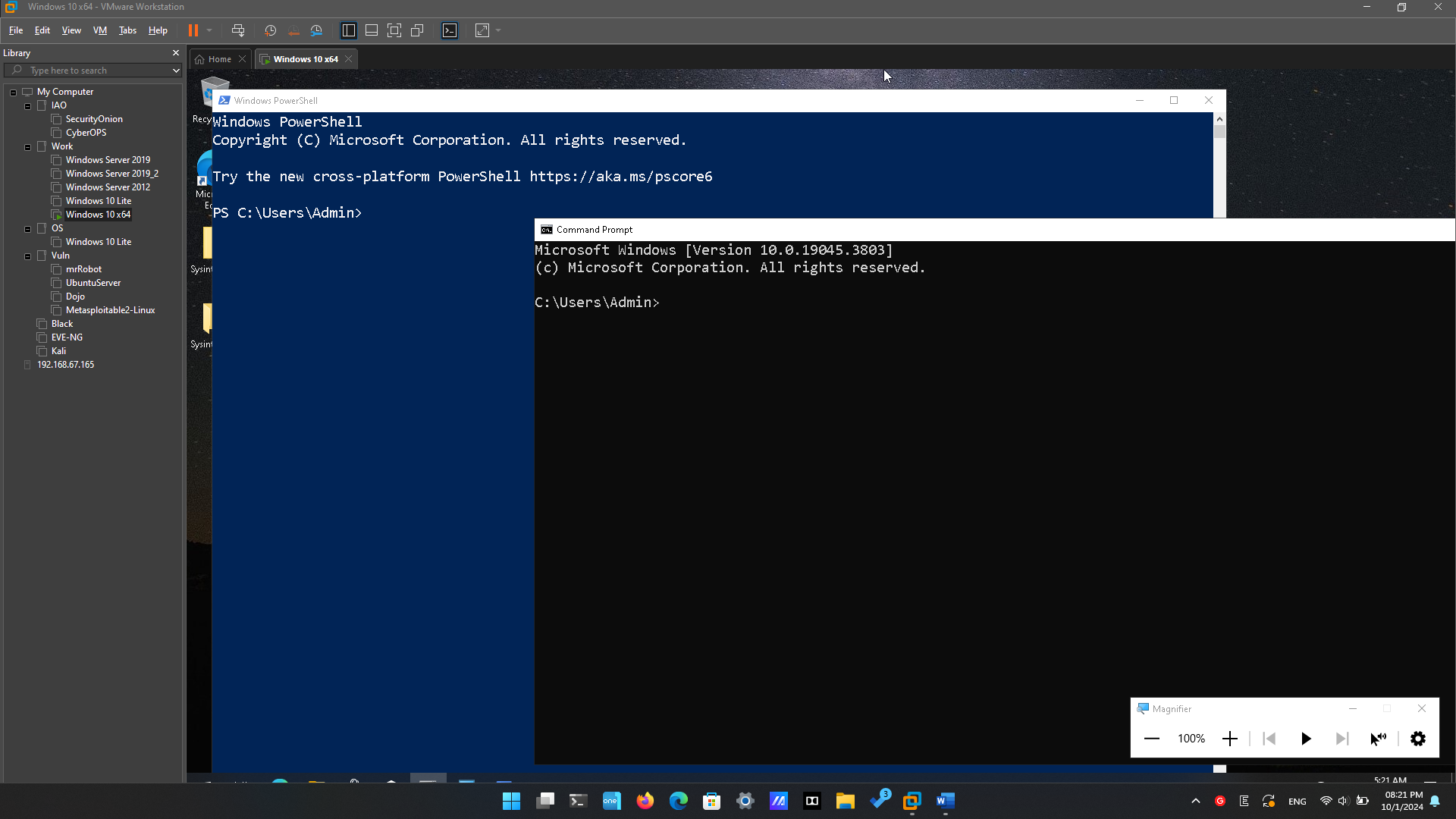
**Lab - Using Windows PowerShell**

# 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, …

A screenshot of a computer

Description automatically generated

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

What are the results?

A screenshot of a computer

Description automatically generated

They also have the same outputs.

## Explore cmdlets.

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

Get-ChildItem

A screenshot of a computer

Description automatically generated

## Explore the netstat command using PowerShell.

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

A computer screen shot of a blue screen

Description automatically generated

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

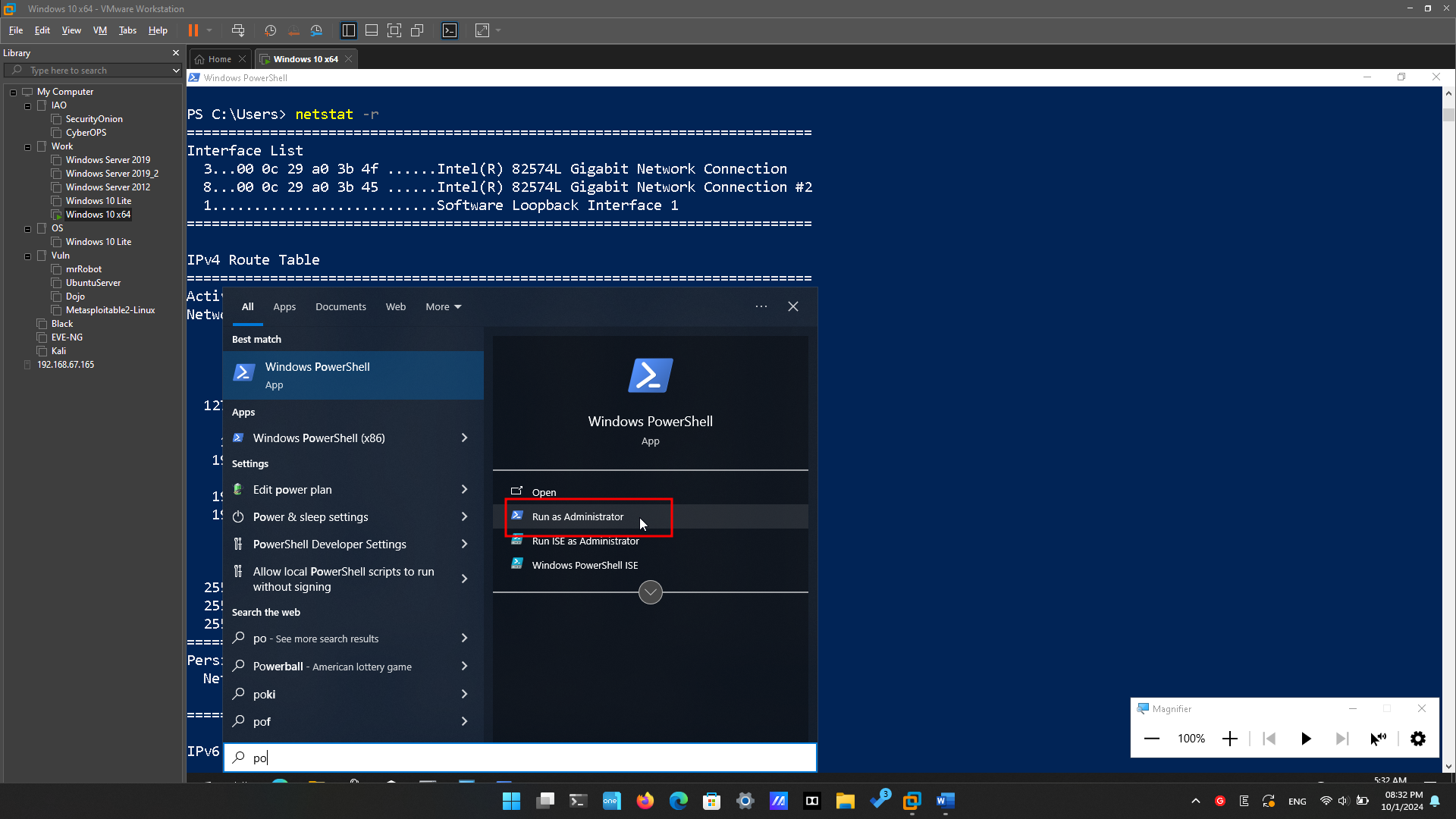
A computer screen shot of a blue screen

Description automatically generated

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.



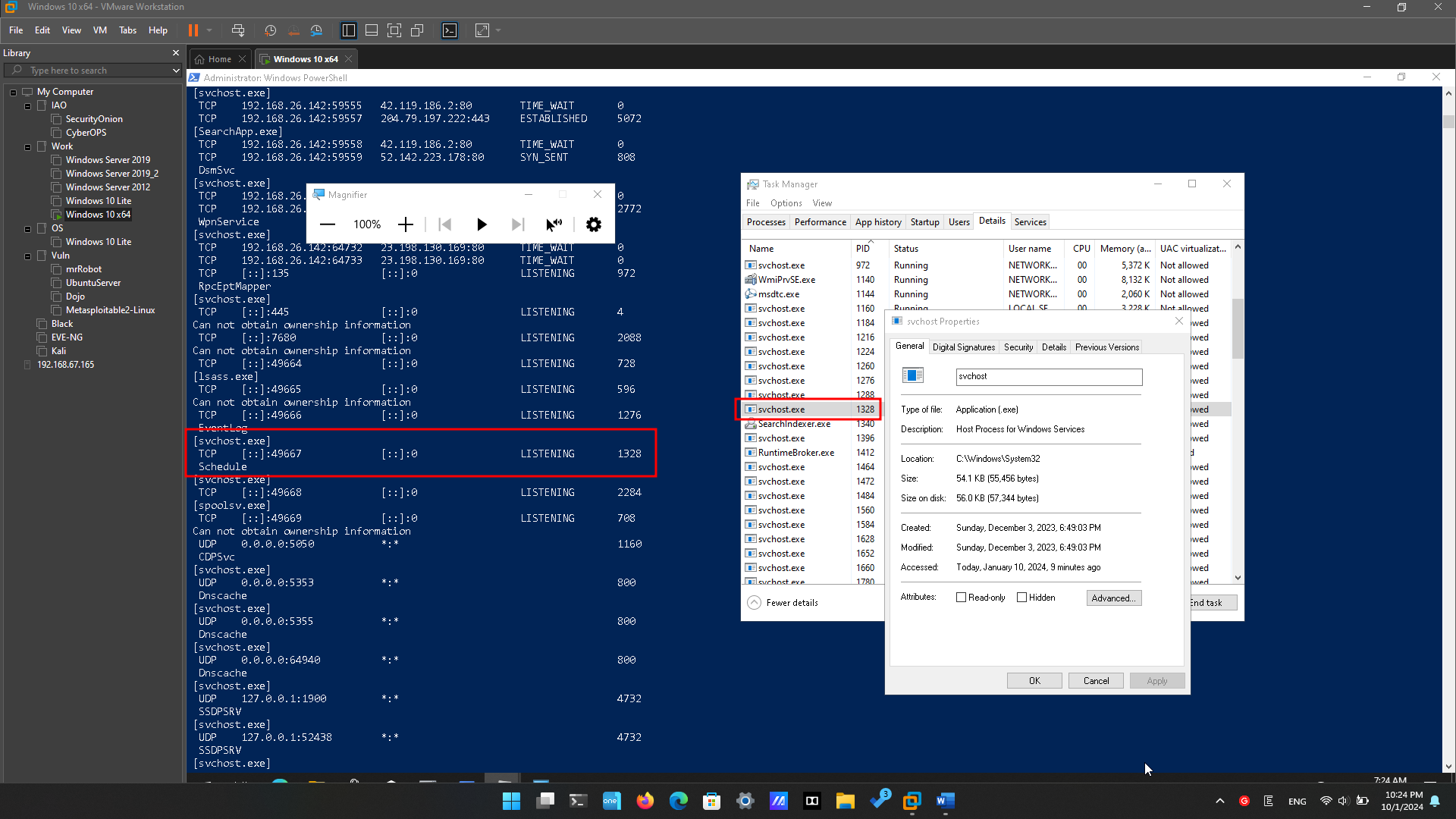
The netstat command can also display the processes associated with the active TCP connections. Enter the **netstat -abno** at the prompt.

A computer screen shot of a blue screen

Description automatically generated

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

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

What happened to the files in the Recycle Bin?

The files in the Recycle Bin are deleted.

# Reflection Question

1. 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

A screenshot of a computer

Description automatically generated

Get-NetFirewallRule:

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

