**PowerShell for Cybersecurity**

Scripting and automation are increasingly sought after skills for IT professionals, including security pros. In this vein, PowerShell is a great choice to get started and set you apart. With the emergence of DevOps in recent years, adding these skills can help propel your career.

If you work in a Windows environment, which most IT professionals do in some capacity, you can start using PowerShell immediately. Whether you are responsible for servers or desktops, you can start using PowerShell to make your job easier. You don’t even need to think like a programmer.

PowerShell is one of the best entry points into programming because it’s widely used and easy to learn. In addition, it’s ideal for gathering information from servers and workstations for audit and compliance purposes.

(*Hacking for Powershell Blue Team*, Powershell: Blue Team Perspective)

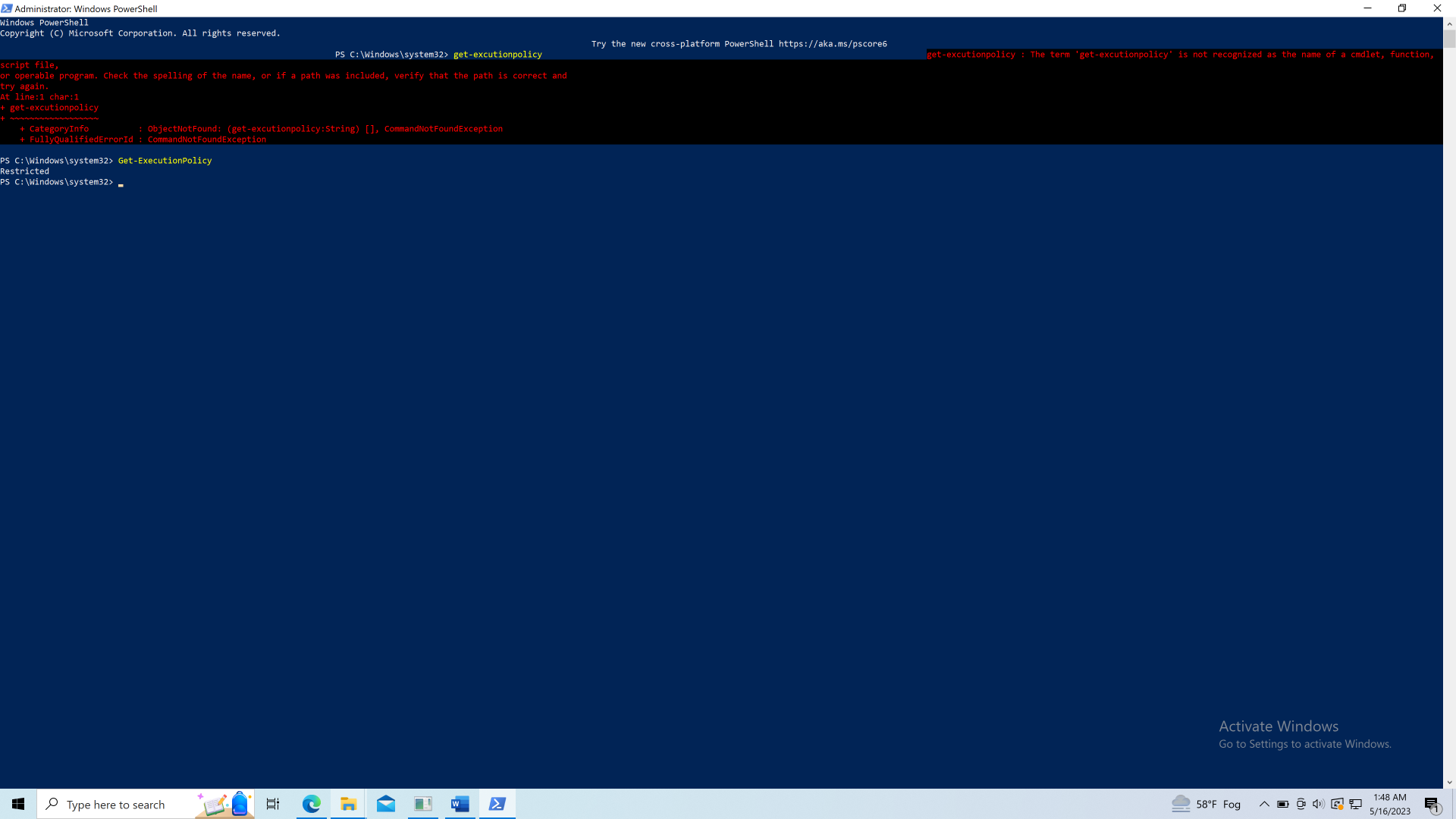
**NOTE:** Unlike Windows, PowerShell does not come preinstalled on Mac. if you are a Mac user, you can install Powershell using the instructions found here: https://techviewleo.com/how-to-install-powershell-on-macos/.

The following exercises are designed to test your knowledge of how to perform certain security-related actions that are routinely carried out by sysadmins and security admins on a regular basis.

In a Google doc, write out the PowerShell command to perform the following exercises. Alternatively, take screenshots of the results on your machine and paste them to the Google doc.

1. Display the current execution policy of PowerShell.  
      
   Execution Policy determines how (or if) PowerShell will run scripts. By default, PowerShell's **execution policy** is set to **Restricted**, meaning that scripts will not run. You can change it using the *Set-ExecutionPolicy* cmdlet. If your policy is set this way, run PowerShell as an Administrator, and change it to “RemoteSigned.”

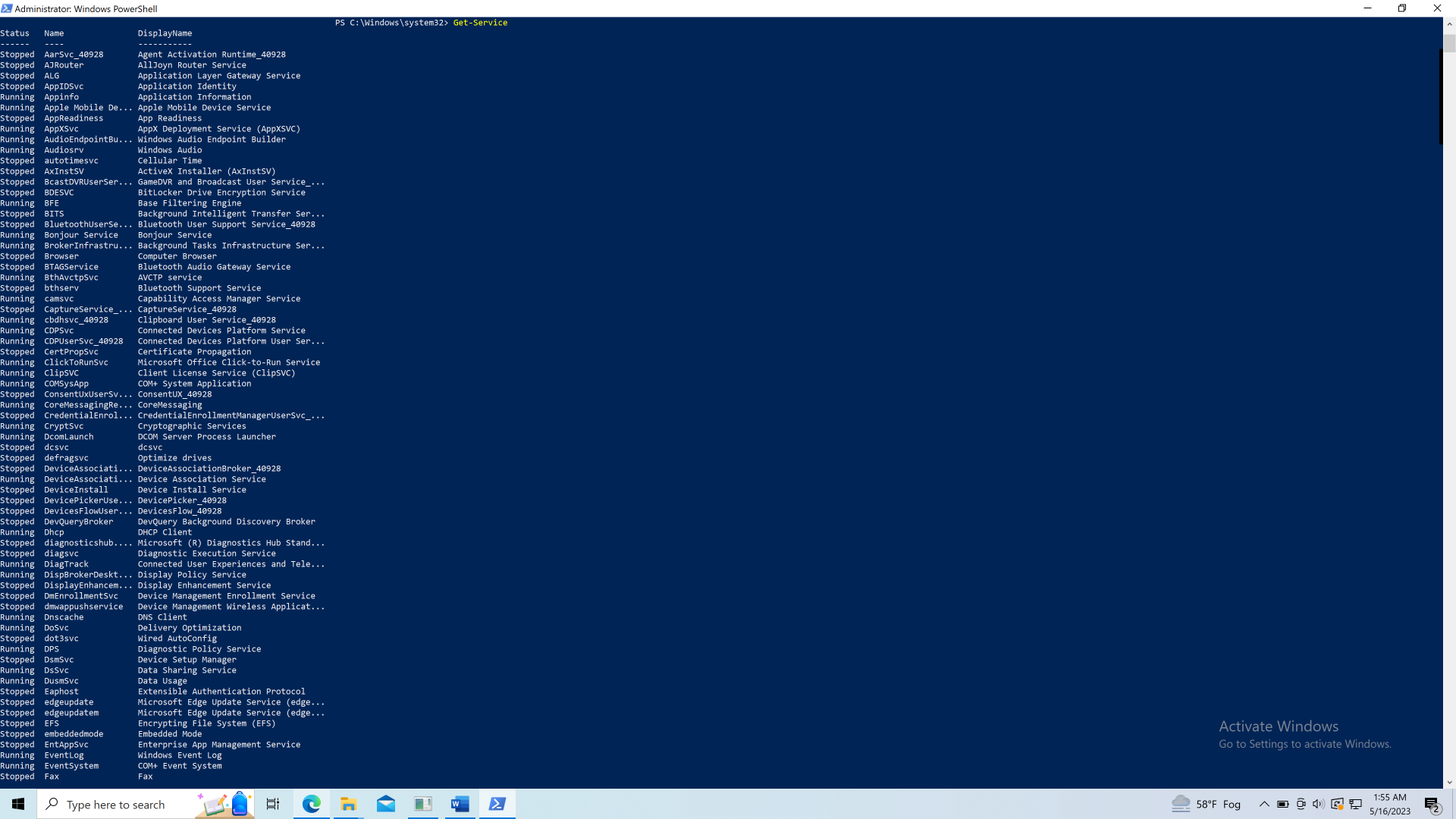
* Get-ExecutionPolicy



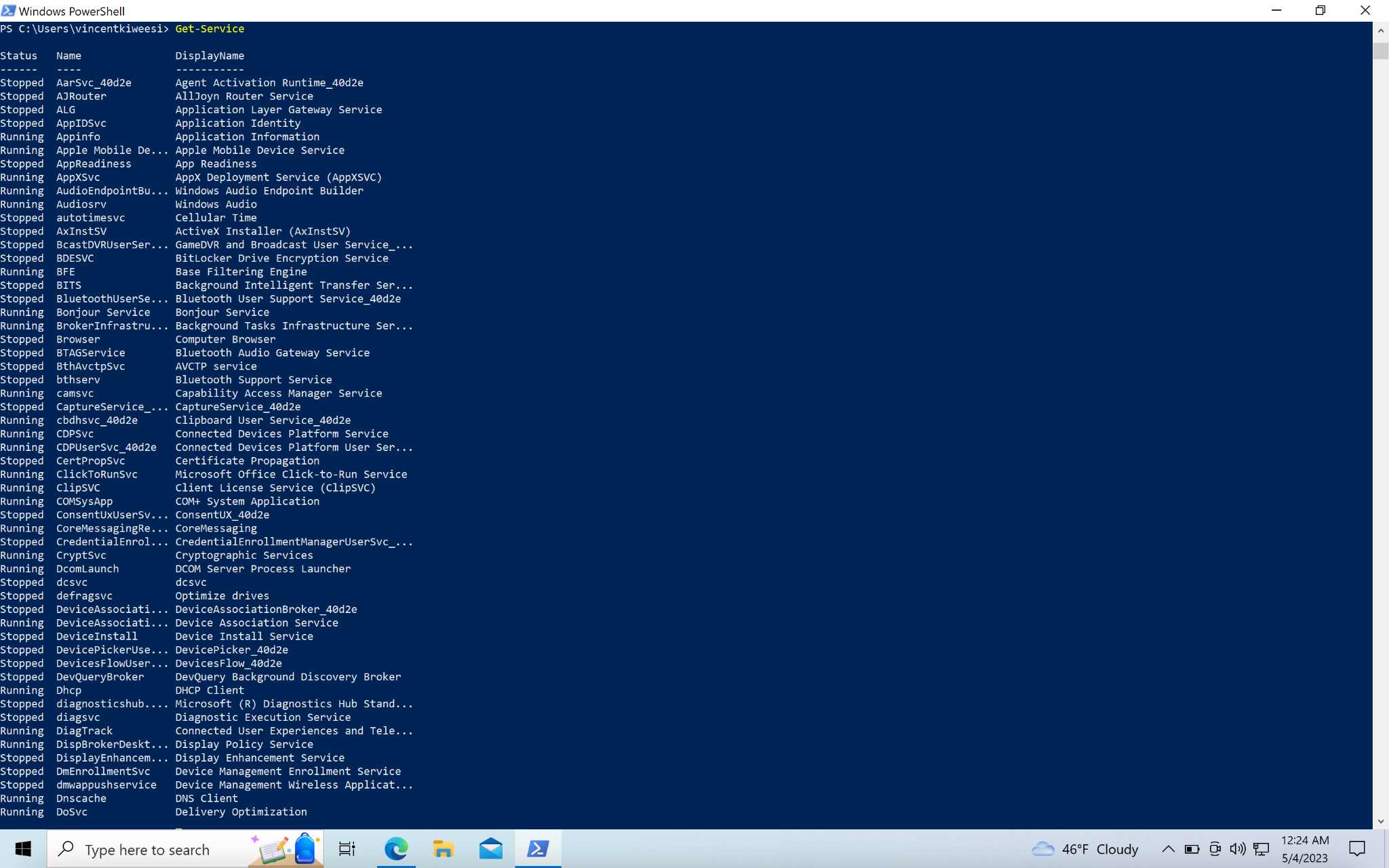
1. Display the current date and time on your machine

* Get-Date 

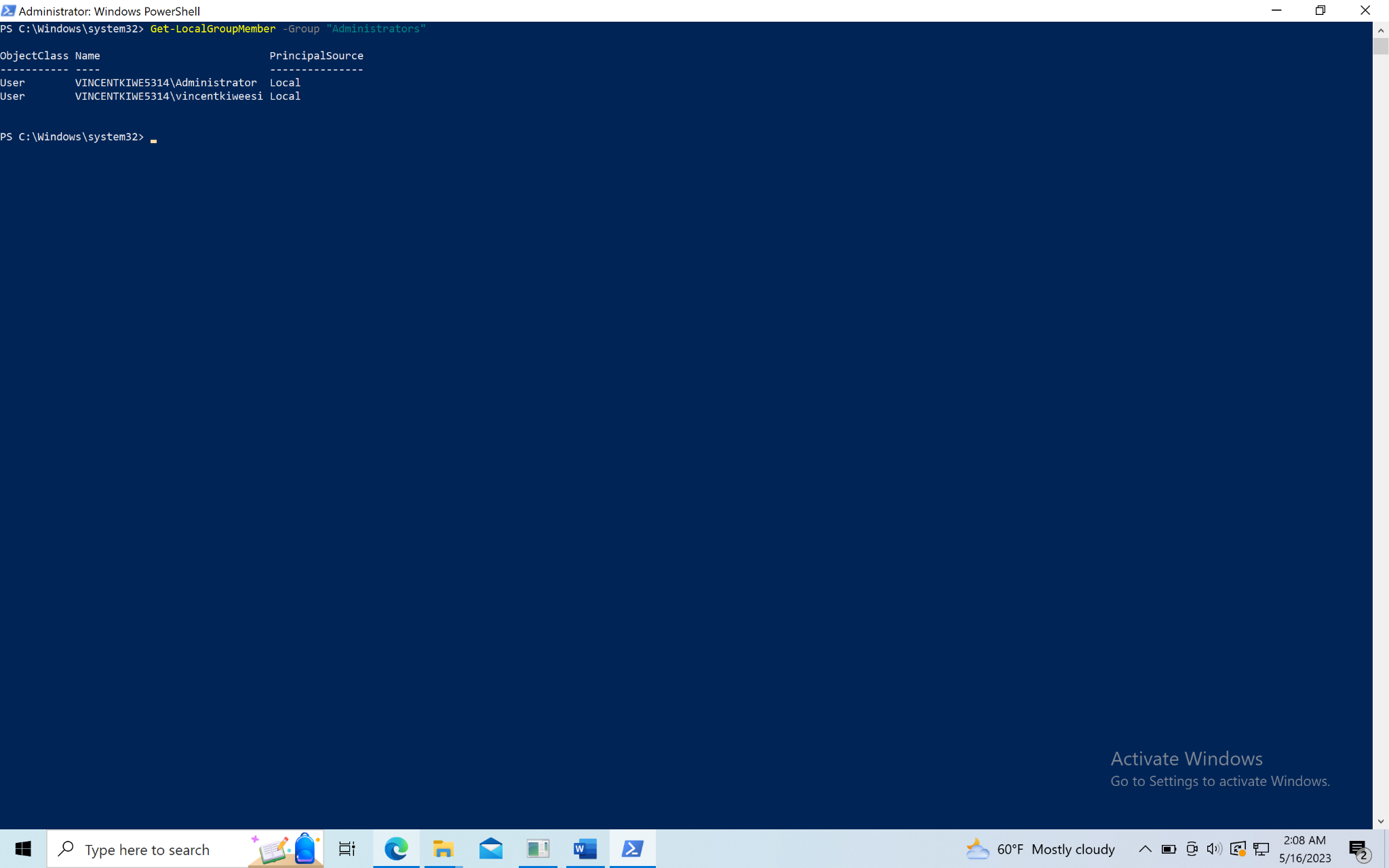
1. List all services on your machine

* Get-Service 

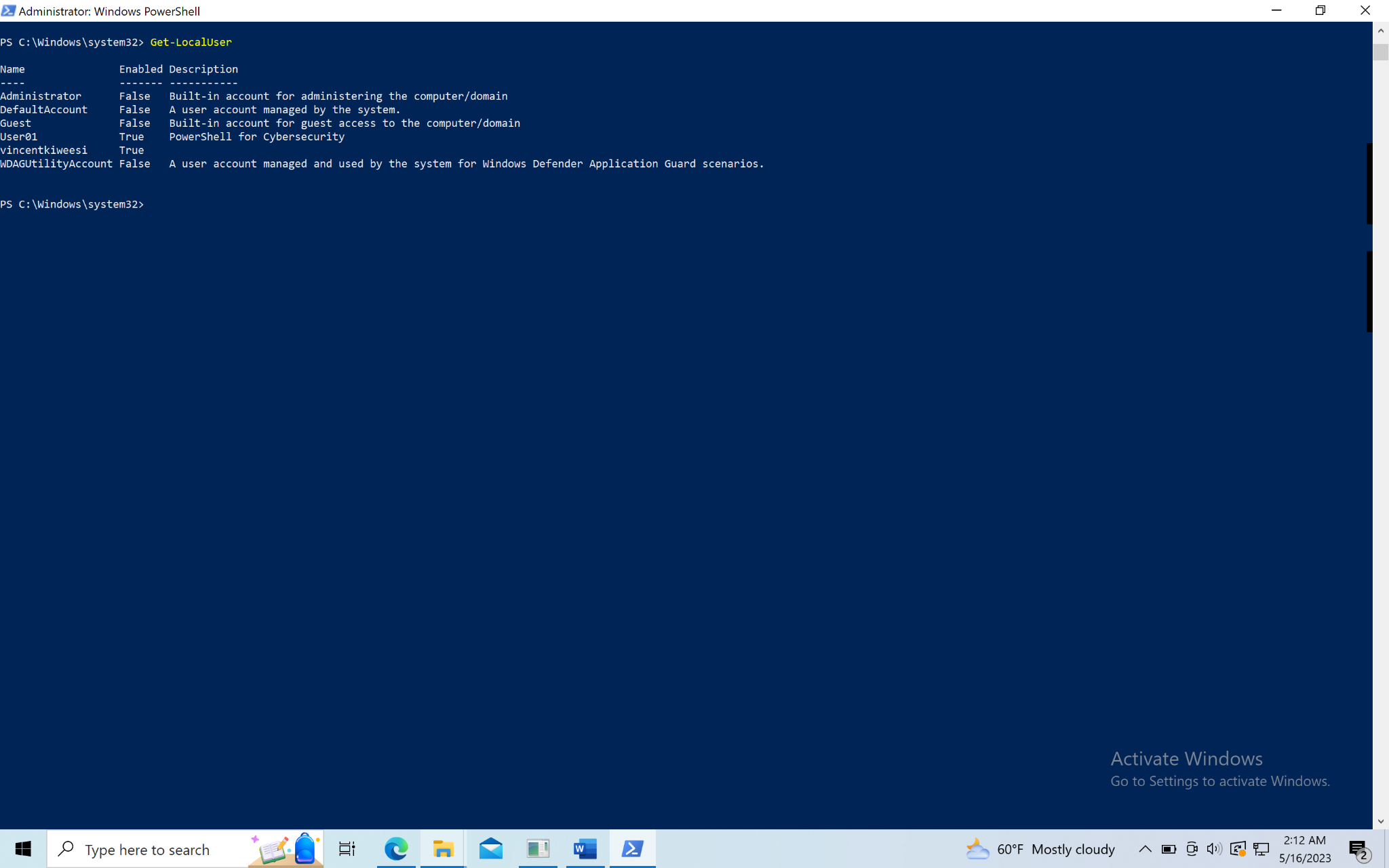
4. List all *running* services on your machine

* Get-Service  
   

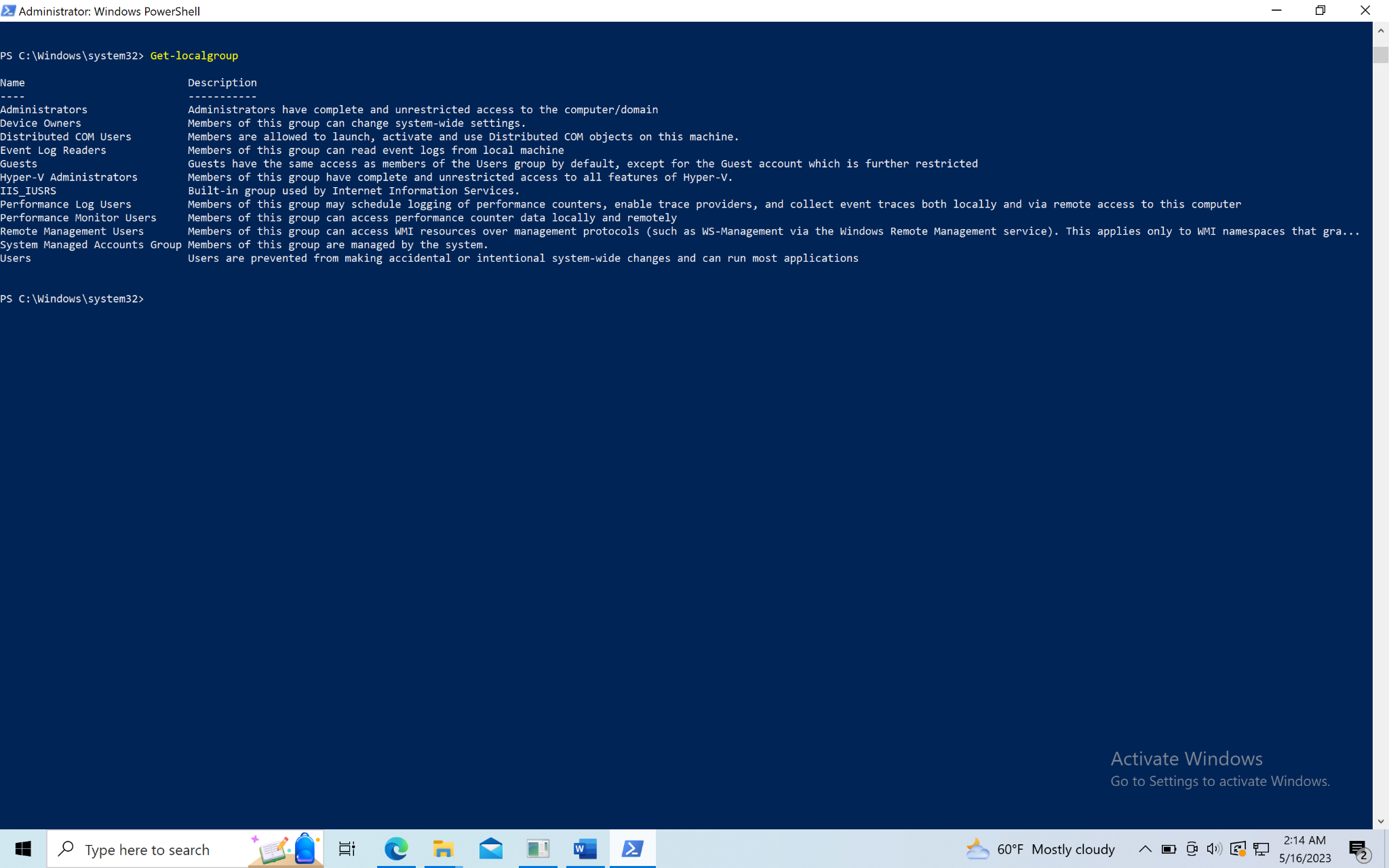
5. List all members of the local Administrators group

* Get-LocalGroupMember -Group "Administrators” 

6. List all users on your machine

Get-LocalUser 

7. List all groups on your machine

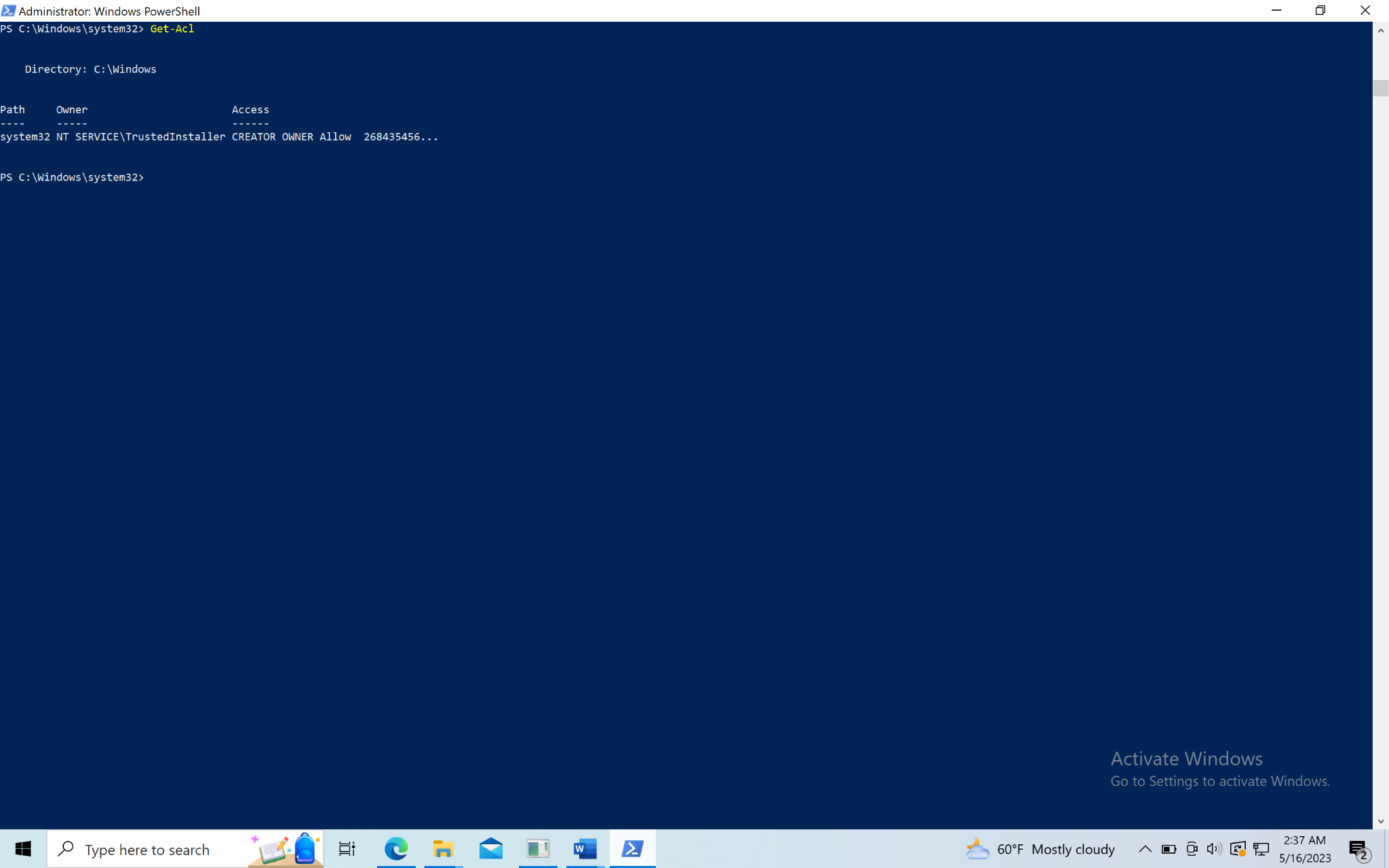
Get-localgroup 

8.Create a new user called *User01*, add a description, and specify no password. Once created, write a script to delete it.

* New-LocalUser -Name User01 -Description "PowerShell for Cybersecurity" -NoPassword
* Remove-LocalUser -Name "User01”  
   

9. Show the security descriptor (acl) of the C:\Windows directory. For Mac users, use the /Users directory.

Get-Acl



10. Create a new file called “test.txt”. Next, add “Hello World!” to the test.txt file. Finally, read the contents of the test.txt file.

