CYBR 1500 Assignment, Week 13+14

# Part I: Required Readings and Lecture Content

Watch the video here:

* **If you don’t have a Windows machine, please watch this video on how to create Windows 10 virtual machine**: <https://www.youtube.com/watch?v=7o26JTFpNrM&feature=youtu.be>

**The website looks a little different from the video, however, the steps should be similar. If you still need help after you watch the video, please feel free to reach out to me.**

Microsoft Windows Free VMs for Development: <https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/>

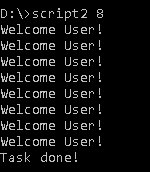
* Week 13 + 14, Update: <https://youtu.be/03XIUUlORys>
* Week 13 + 14, lecture 1: <https://youtu.be/goFR0LUHn9Q>
* Week 13 + 14, lecture 2: <https://youtu.be/e17zRdUogX0>
* Week 13 + 14, lecture 3: <https://youtu.be/OsgRGqBleRc>
* Week 13 + 14, lecture 4: <https://youtu.be/gAtpCs_3nv0>
* Week 13 + 14, lecture 5: [https://youtu.be/u7xdYazIdGU](%20https:/youtu.be/u7xdYazIdGU)

# Part 2: **Windows Command Prompt** (30 points)

**Please perform these instructions in Window Command Prompt:**

1. Create a directory called **CYBR\_1500**.
2. Under **CYBR\_1500**, create a directory called **Exercise**.
3. Under **Exercise** directory, please create a **Scripts** directory.
4. Under **Scripts** directory, please create **script1.cmd** with the text content “Hello, this is script1”. **Then run the script.**
5. Under **Scripts** directory, create a **script2.cmd** using notepad/sublime text. This script will read the user input then display the message “Welcome User!” as many times as the user’s input. For example: if the user’s input is 6 then the script will display the message 6 times. **Then run the script.**

Below is the sample output of the script:



Please make sure capture the terminal interactions below.

>>>>>Paste your terminal capture below this line >>>>>

C:\Users\Andrew\CYBR\_1500\Exercise\Scripts>script1

Hello, this is script1

C:\Users\Andrew\CYBR\_1500\Exercise\Scripts>script2 7

Welcome User!

Welcome User!

Welcome User!

Welcome User!

Welcome User!

Welcome User!

Welcome User!

Task done!

C:\Users\Andrew\CYBR\_1500\Exercise\Scripts>script2 4

Welcome User!

Welcome User!

Welcome User!

Welcome User!

Task done!

C:\Users\Andrew\CYBR\_1500\Exercise\Scripts>

<<<<< Paste your terminal capture above this line <<<<<

# Part 3: **Windows PowerShell** (30 points)

**Please perform these instructions in Windows PowerShell:**

1. From your current working directory, use the appropriate command to list all the files and directories.
2. Use the appropriate command to change directory one level above your current working directory e.g. from C:\Users\trang to C:\Users
3. Using the appropriate command to test connection with your local host (ping)
4. Change directory to HKCU dric (Hkey\_Current\_User) and list the content in HKCU.
5. From HKCU, list all the contents of software directories
6. Use the appropriate command to get PSDrive
7. List all the contents of Variable directory
8. Use the appropriate command to display the version of your Windows PowerShell
9. Use appropriate command to display all the commands in PowerShell related to Event (in other words, all the commands that contain the word “event”)
10. Use the appropriate command to find information about Get-EventLog
11. Use one command to list all the content in C:\Program Files
12. Come back to your home directory, which should be something like C:\Users\<your name>, mine is C:\Users\Trang Horn.
13. Create a file with name file1.txt with the following content using notepad:

Hello world!

This is a test.

1. Read file1.txt using three different ways.
2. Use the appropriate command to get the services of your local host.

Please make sure capture the terminal interactions or the commands used for each step below

>>>>>Paste your terminal capture below this line >>>>>

PS C:\Users\andrew> dir

Directory: C:\Users\andrew

Mode LastWriteTime Length Name

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

d----- 4/12/2022 4:12 AM .VirtualBox

d----- 4/2/2022 12:50 AM ansel

d-r--- 3/30/2022 7:19 PM Contacts

d----- 4/24/2022 5:48 PM CYBR\_1500

d-r--- 4/24/2022 7:42 PM Desktop

d-r--- 4/23/2022 12:28 AM Documents

d-r--- 4/24/2022 6:11 PM Downloads

d-r--- 3/30/2022 7:19 PM Favorites

d-r--- 3/30/2022 7:19 PM Links

d-r--- 3/30/2022 7:19 PM Music

dar--l 4/24/2022 1:00 PM OneDrive

d-r--- 3/30/2022 7:20 PM Pictures

d-r--- 4/1/2022 9:30 PM Saved Games

d-r--- 3/30/2022 5:39 PM Searches

d-r--- 4/2/2022 12:52 AM Videos

d----- 3/31/2022 1:25 AM VirtualBox VMs

-a---- 3/30/2022 6:39 PM 2702 AMDRM\_Install.log

-a---- 3/30/2022 6:39 PM 2727498 AMD\_RyzenMaster.log

PS C:\Users\andrew> cd ..

PS C:\Users> ping localhost

Pinging AndrewPC [::1] with 32 bytes of data:

Reply from ::1: time<1ms

Reply from ::1: time<1ms

Reply from ::1: time<1ms

Reply from ::1: time<1ms

Ping statistics for ::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> cd HKCU

cd : Cannot find path 'C:\Users\HKCU' because it does not exist.

At line:1 char:1

+ cd HKCU

+ ~~~~~~~

+ CategoryInfo : ObjectNotFound: (C:\Users\HKCU:String) [Set-Location], ItemNotFoundExc

eption

+ FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.SetLocationCommand

PS C:\Users> cd HKCU:

PS HKCU:\> ls

Hive: HKEY\_CURRENT\_USER

Name Property

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

AppEvents

Console ColorTable00 : 789516

ColorTable01 : 14300928

ColorTable02 : 958739

ColorTable03 : 14521914

ColorTable04 : 2035653

ColorTable05 : 9967496

ColorTable06 : 40129

ColorTable07 : 13421772

ColorTable08 : 7763574

ColorTable09 : 16742459

ColorTable10 : 837142

ColorTable11 : 14079585

ColorTable12 : 5654759

ColorTable13 : 10354868

ColorTable14 : 10875385

ColorTable15 : 15921906

CtrlKeyShortcutsDisabled : 0

CursorColor : 4294967295

CursorSize : 25

DefaultBackground : 4294967295

DefaultForeground : 4294967295

EnableColorSelection : 0

ExtendedEditKey : 1

ExtendedEditKeyCustom : 0

FaceName : \_\_DefaultTTFont\_\_

FilterOnPaste : 1

FontFamily : 0

FontSize : 1048576

FontWeight : 0

ForceV2 : 1

FullScreen : 0

HistoryBufferSize : 50

HistoryNoDup : 0

InsertMode : 1

LineSelection : 1

LineWrap : 1

LoadConIme : 1

NumberOfHistoryBuffers : 4

PopupColors : 245

QuickEdit : 1

ScreenBufferSize : 589889656

ScreenColors : 7

ScrollScale : 1

TerminalScrolling : 0

TrimLeadingZeros : 0

WindowAlpha : 255

WindowSize : 1966200

WordDelimiters : 0

Control Panel SettingsExtensionAppSnapshot : {0, 0, 0, 0...}

Environment Path :

C:\Users\Andrew\AppData\Local\Microsoft\WindowsApps;

TEMP : C:\Users\Andrew\AppData\Local\Temp

TMP : C:\Users\Andrew\AppData\Local\Temp

OneDrive : C:\Users\Andrew\OneDrive

OneDriveConsumer : C:\Users\Andrew\OneDrive

EUDC

Keyboard Layout

Network

Printers

Software

System

Uninstall

Volatile Environment LOGONSERVER : \\ANDREWPC

USERDOMAIN : ANDREWPC

USERNAME : Andrew

USERPROFILE : C:\Users\Andrew

HOMEPATH : \Users\Andrew

HOMEDRIVE : C:

APPDATA : C:\Users\Andrew\AppData\Roaming

LOCALAPPDATA : C:\Users\Andrew\AppData\Local

USERDOMAIN\_ROAMINGPROFILE : ANDREWPC

PS HKCU:\> cd software

PS HKCU:\software> ls

Hive: HKEY\_CURRENT\_USER\software

Name Property

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

A-Volute

AppDataLow

Battlestate Games

Blizzard Entertainment

ChangeTracker

Chromium

Corsair

Discord

ENE\_RGB\_HAL\_QSI\_Loki HAL Version : {1,0,3,0 200610}

Count : {0, 쪰ৃ̓灰, ǉ☺, ...}

Epic Games

f7c32559-6c31-590a-9972-0bea54 InstallLocation : C:\Users\Andrew\AppData\Local\Programs\nordpass

b04213 KeepShortcuts : true

ShortcutName : NordPass

MenuDirectory : NordSec

Gaijin

Google

Logitech

Ludeon Studios

Microsoft

Mojang

MSI

Netscape

NVIDIA Corporation

ODBC

Oracle

Policies

QtProject

RegisteredApplications AppXk7cmaptv7892fde8mnck1fk8yypwb11a : Software\Classes\Local

Settings\Software\Microsoft\Windows\Cur

rentVersion\AppModel\Repository\Packages\Microsoft.Windows.Clo

udExperienceHost\_10.0.22000.1\_neutral\_neutral\_cw5n1h2txyewy\Ap

p\Capabilities

AppX0m1r2p2r050dfvf92x6mzb6ry9w1yyxh : Software\Classes\Local

Settings\Software\Microsoft\Windows\Cur

rentVersion\AppModel\Repository\Packages\Microsoft.AAD.BrokerP

lugin\_1000.19580.1000.0\_neutral\_neutral\_cw5n1h2txyewy\App\Capa

bilities

AppXsact8rq2t1kzyzpajdeyezsqr9fd921x : Software\Classes\Local

Settings\Software\Microsoft\Windows\Cur

rentVersion\AppModel\Repository\Packages\Microsoft.Windows.OOB

ENetworkConnectionFlow\_10.0.21302.1000\_neutral\_\_cw5n1h2txyewy\

App\Capabilities

AppXpr50p668ddzpme2as177qfjp6mbfpphs : Software\Classes\Local

Settings\Software\Microsoft\Windows\Cur

rentVersion\AppModel\Repository\Packages\Microsoft.Windows.OOB

ENetworkCaptivePortal\_10.0.21302.1000\_neutral\_\_cw5n1h2txyewy\A

pp\Capabilities

AppXh8ha6ytjh9k9ghjv882fypn2phma0km5 : Software\Classes\Local

Settings\Software\Microsoft\Windows\Cur

rentVersion\AppModel\Repository\Packages\MicrosoftWindows.Clie

nt.CBS\_1000.22000.318.0\_x64\_\_cw5n1h2txyewy\WebExperienceHost\C

apabilities

AppXaxqsajj9cvbefhtkafjkh7qwg16365xx : Software\Classes\Local

Settings\Software\Microsoft\Windows\Cur

rentVersion\AppModel\Repository\Packages\MicrosoftWindows.Clie

nt.CBS\_1000.22000.318.0\_x64\_\_cw5n1h2txyewy\CortanaUI\Capabilit

ies

AppXmptrsdhnzvzyf4487waxwnbswpsgrpxf : Software\Classes\Local

Settings\Software\Microsoft\Windows\Cur

rentVersion\AppModel\Repository\Packages\MicrosoftWindows.Clie

nt.CBS\_1000.22000.318.0\_x64\_\_cw5n1h2txyewy\ScreenClipping\Capa

bilities

AppXvrm09rf74wmxmnk402kr59cpd7efwk0t : Software\Classes\Local

Settings\Software\Microsoft\Windows\Cur

rentVersion\AppModel\Repository\Packages\MicrosoftWindows.Clie

nt.CBS\_1000.22000.318.0\_x64\_\_cw5n1h2txyewy\InputApp\Capabiliti

es

AppXp86v8cghwd0yp385zqxj81c96t5r955y : Software\Classes\Local

Settings\Software\Microsoft\Windows\Cur

rentVersion\AppModel\Repository\Packages\Microsoft.MicrosoftEd

ge\_44.22000.120.0\_neutral\_\_8wekyb3d8bbwe\MicrosoftEdge\Capabil

ities

AppX6nja9x2egvt2qx1bbjypndsrt2ay5398 : Software\Classes\Local

Settings\Software\Microsoft\Windows\Cur

rentVersion\AppModel\Repository\Packages\microsoft.windowscomm

unicationsapps\_16005.12827.20400.0\_x64\_\_8wekyb3d8bbwe\microsof

t.windowslive.manageaccounts\Capabilities

AppXp1x3ca98sr04xrb97rcdcdfhpcqznejh : Software\Classes\Local

Settings\Software\Microsoft\Windows\Cur

rentVersion\AppModel\Repository\Packages\microsoft.windowscomm

unicationsapps\_16005.12827.20400.0\_x64\_\_8wekyb3d8bbwe\microsof

t.windowslive.calendar\Capabilities

AppXfgqtaeqtqrb2q2dk1x91pgkg3zh7kk7g : Software\Classes\Local

Settings\Software\Microsoft\Windows\Cur

rentVersion\AppModel\Repository\Packages\microsoft.windowscomm

unicationsapps\_16005.12827.20400.0\_x64\_\_8wekyb3d8bbwe\microsof

t.windowslive.mail\Capabilities

AppXpvggj8wtagvqq1trs4afp513ydqb63tt : Software\Classes\Local

Settings\Software\Microsoft\Windows\Cur

rentVersion\AppModel\Repository\Packages\Windows.PrintDialog\_6

.2.1.0\_neutral\_neutral\_cw5n1h2txyewy\Microsoft.Windows.PrintDi

alog\Capabilities

AppXw0vccgbg3r3rkvs0jbxgc9wq1hntgxgz : Software\Classes\Local

Settings\Software\Microsoft\Windows\Cur

rentVersion\AppModel\Repository\Packages\Microsoft.XboxGameCal

...

Santa Goat

Spotify

SyncEngines

Team17 Digital Limited

Team17 Digital Ltd

Unwinder

Valve

Wow6432Node

Youthcat Studio

Classes

PS HKCU:\software> cd C:\Users\Andrew\

PS C:\Users\Andrew> Get-PSDrive

Name Used (GB) Free (GB) Provider Root CurrentLocat

ion

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

Alias Alias

C 366.50 1495.81 FileSystem C:\ Users\Andrew

Cert Certificate \

D 61.21 3664.69 FileSystem D:\

Env Environment

Function Function

HKCU Registry HKEY\_CURRENT\_USER software

HKLM Registry HKEY\_LOCAL\_MACHINE

Variable Variable

WSMan WSMan

PS C:\Users\Andrew> dir Variable:

Name Value

---- -----

$ Get-PSDrive

? True

^ Get-PSDrive

args {}

ConfirmPreference High

ConsoleFileName

DebugPreference SilentlyContinue

Error {Cannot find path 'C:\Users\HKCU' because it does not exist., Canno...

ErrorActionPreference Continue

ErrorView NormalView

ExecutionContext System.Management.Automation.EngineIntrinsics

false False

FormatEnumerationLimit 4

HOME C:\Users\Andrew

Host System.Management.Automation.Internal.Host.InternalHost

InformationPreference SilentlyContinue

input System.Collections.ArrayList+ArrayListEnumeratorSimple

LASTEXITCODE 0

MaximumAliasCount 4096

MaximumDriveCount 4096

MaximumErrorCount 256

MaximumFunctionCount 4096

MaximumHistoryCount 4096

MaximumVariableCount 4096

MyInvocation System.Management.Automation.InvocationInfo

NestedPromptLevel 0

null

OutputEncoding System.Text.ASCIIEncoding

PID 21028

PROFILE C:\Users\Andrew\Documents\WindowsPowerShell\Microsoft.PowerShell\_pr...

ProgressPreference Continue

PSBoundParameters {}

PSCommandPath

PSCulture en-US

PSDefaultParameterValues {}

PSEdition Desktop

PSEmailServer

PSHOME C:\Windows\System32\WindowsPowerShell\v1.0

PSScriptRoot

PSSessionApplicationName wsman PSSessionConfigurationName http://schemas.microsoft.com/powershell/Microsoft.PowerShell PSSessionOption System.Management.Automation.Remoting.PSSessionOption PSUICulture en-US PSVersionTable {PSVersion, PSEdition, PSCompatibleVersions, BuildVersion...} PWD C:\Users\Andrew

ShellId Microsoft.PowerShell

StackTrace at System.Management.Automation.CommandDiscovery.LookupCommandIn...

true True

VerbosePreference SilentlyContinue

WarningPreference Continue

WhatIfPreference False

PS C:\Users\Andrew> $PSVersiontable

Name Value

---- -----

PSVersion 5.1.22000.613

PSEdition Desktop

PSCompatibleVersions {1.0, 2.0, 3.0, 4.0...}

BuildVersion 10.0.22000.613

CLRVersion 4.0.30319.42000

WSManStackVersion 3.0

PSRemotingProtocolVersion 2.3

SerializationVersion 1.1.0.1

PS C:\Users\Andrew> help \*event\*

Name Category Module Synopsis

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

Clear-EventLog Cmdlet Microsoft.PowerShell.M... ...

Get-EventLog Cmdlet Microsoft.PowerShell.M... ...

Limit-EventLog Cmdlet Microsoft.PowerShell.M... ...

New-EventLog Cmdlet Microsoft.PowerShell.M... ...

Register-WmiEvent Cmdlet Microsoft.PowerShell.M... ...

Remove-EventLog Cmdlet Microsoft.PowerShell.M... ...

Show-EventLog Cmdlet Microsoft.PowerShell.M... ...

Write-EventLog Cmdlet Microsoft.PowerShell.M... ...

Get-Event Cmdlet Microsoft.PowerShell.U... ...

Get-EventSubscriber Cmdlet Microsoft.PowerShell.U... ...

New-Event Cmdlet Microsoft.PowerShell.U... ...

Register-EngineEvent Cmdlet Microsoft.PowerShell.U... ...

Register-ObjectEvent Cmdlet Microsoft.PowerShell.U... ...

Remove-Event Cmdlet Microsoft.PowerShell.U... ...

Unregister-Event Cmdlet Microsoft.PowerShell.U... ...

Wait-Event Cmdlet Microsoft.PowerShell.U... ...

Register-CimIndicationEvent Cmdlet CimCmdlets ...

Get-WinEvent Cmdlet Microsoft.PowerShell.D... Get-WinEvent...

New-WinEvent Cmdlet Microsoft.PowerShell.D... New-WinEvent...

Enable-BcdElementEventLogging Cmdlet Microsoft.Windows.Bcd.... Enable-BcdElementEventLoggin...

Disable-BcdElementEventLogging Cmdlet Microsoft.Windows.Bcd.... Disable-BcdElementEventLoggi...

Remove-NetEventVmSwitchProvider Function NetEventPacketCapture ...

Remove-NetEventPacketCapturePr... Function NetEventPacketCapture ...

Get-NetEventVmSwitchProvider Function NetEventPacketCapture ...

Add-NetEventVFPProvider Function NetEventPacketCapture ...

Remove-NetEventVFPProvider Function NetEventPacketCapture ...

Get-NetEventVmNetworkAdapter Function NetEventPacketCapture ...

Get-NetEventVmSwitch Function NetEventPacketCapture ...

Add-NetEventNetworkAdapter Function NetEventPacketCapture ...

Get-NetEventNetworkAdapter Function NetEventPacketCapture ...

Get-NetEventProvider Function NetEventPacketCapture ...

Add-NetEventVmSwitchProvider Function NetEventPacketCapture ...

Stop-NetEventSession Function NetEventPacketCapture ...

Add-NetEventVmNetworkAdapter Function NetEventPacketCapture ...

Add-NetEventVmSwitch Function NetEventPacketCapture ...

Get-NetEventSession Function NetEventPacketCapture ...

Set-NetEventProvider Function NetEventPacketCapture ...

Remove-NetEventNetworkAdapter Function NetEventPacketCapture ...

Start-NetEventSession Function NetEventPacketCapture ...

Get-NetEventPacketCaptureProvider Function NetEventPacketCapture ...

Set-NetEventVmSwitchProvider Function NetEventPacketCapture ...

Set-NetEventVFPProvider Function NetEventPacketCapture ...

Remove-NetEventVmNetworkAdapter Function NetEventPacketCapture ...

Remove-NetEventProvider Function NetEventPacketCapture ...

Add-NetEventProvider Function NetEventPacketCapture ...

Get-NetEventVFPProvider Function NetEventPacketCapture ...

Set-NetEventPacketCaptureProvider Function NetEventPacketCapture ...

Add-NetEventPacketCaptureProvider Function NetEventPacketCapture ...

Get-NetEventWFPCaptureProvider Function NetEventPacketCapture ...

New-NetEventSession Function NetEventPacketCapture ...

Add-NetEventWFPCaptureProvider Function NetEventPacketCapture ...

Set-NetEventSession Function NetEventPacketCapture ...

Remove-NetEventSession Function NetEventPacketCapture ...

Remove-NetEventVmSwitch Function NetEventPacketCapture ...

Set-NetEventWFPCaptureProvider Function NetEventPacketCapture ...

Remove-NetEventWFPCaptureProvider Function NetEventPacketCapture ...

PS C:\Users\Andrew>

PS C:\Users\Andrew>

PS C:\Users\Andrew>

PS C:\Users\Andrew>

PS C:\Users\Andrew>

PS C:\Users\Andrew>

PS C:\Users\Andrew>

PS C:\Users\Andrew>

PS C:\Users\Andrew>

PS C:\Users\Andrew>

PS C:\Users\Andrew>

PS C:\Users\Andrew>

PS C:\Users\Andrew> help Get-EventLog

NAME

Get-EventLog

SYNTAX

Get-EventLog [-LogName] <string> [[-InstanceId] <long[]>] [-ComputerName <string[]>] [-Newest

<int>] [-After <datetime>] [-Before <datetime>] [-UserName <string[]>] [-Index <int[]>]

[-EntryType {Error | Information | FailureAudit | SuccessAudit | Warning}] [-Source <string[]>]

[-Message <string>] [-AsBaseObject] [<CommonParameters>]

Get-EventLog [-ComputerName <string[]>] [-List] [-AsString] [<CommonParameters>]

ALIASES

None

REMARKS

Get-Help cannot find the Help files for this cmdlet on this computer. It is displaying only

partial help.

-- To download and install Help files for the module that includes this cmdlet, use

Update-Help.

-- To view the Help topic for this cmdlet online, type: "Get-Help Get-EventLog -Online" or

go to https://go.microsoft.com/fwlink/?LinkID=113314.

PS C:\Users\Andrew> dir 'C:\Program Files\'

Directory: C:\Program Files

Mode LastWriteTime Length Name

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

d----- 3/30/2022 6:39 PM AMD

d----- 3/30/2022 9:45 PM Common Files

d----- 3/31/2022 2:47 AM Corsair

d----- 3/30/2022 8:13 PM ENE

d----- 3/30/2022 6:59 PM EqualizerAPO

d----- 3/30/2022 5:45 PM Google

d----- 11/4/2021 9:27 AM Internet Explorer

d----- 4/14/2022 9:42 PM LGHUB

d----- 4/23/2022 11:44 PM Microsoft Office

d----- 3/30/2022 8:58 PM Microsoft Office 15

d----- 4/18/2022 10:20 PM Microsoft OneDrive

d----- 4/5/2022 9:40 PM Microsoft Update Health Tools

d----- 6/5/2021 7:10 AM ModifiableWindowsApps

d----- 4/1/2022 11:49 AM NordUpdater

d----- 4/9/2022 10:00 PM NordVPN

d----- 3/30/2022 6:27 PM NVIDIA Corporation

d----- 3/31/2022 12:34 AM Oracle

d----- 4/24/2022 6:12 PM Sublime Text

d----- 3/30/2022 8:13 PM WD

d----- 3/30/2022 6:09 PM Windows Defender

d----- 3/30/2022 5:38 PM Windows Defender Advanced Threat Protection

d----- 11/4/2021 9:27 AM Windows Mail

d----- 3/30/2022 5:38 PM Windows Media Player

d----- 6/5/2021 9:21 AM Windows NT

d----- 11/4/2021 9:27 AM Windows Photo Viewer

d----- 6/5/2021 7:10 AM WindowsPowerShell

PS C:\Users\Andrew> notepad file1.txt

PS C:\Users\Andrew> notepad file1.txt

PS C:\Users\Andrew> notepad file1.txt

PS C:\Users\Andrew> type .\file1.txt

local host

server

Hello world!

This is a test.

PS C:\Users\Andrew> Get-Service -ComputerName localhost

Status Name DisplayName

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

Stopped AarSvc\_265e608d Agent Activation Runtime\_265e608d

Stopped AJRouter AllJoyn Router Service

Stopped ALG Application Layer Gateway Service

Stopped AppIDSvc Application Identity

Running Appinfo Application Information

Stopped AppMgmt Application Management

Stopped AppReadiness App Readiness

Stopped AppVClient Microsoft App-V Client

Running AppXSvc AppX Deployment Service (AppXSVC)

Stopped AssignedAccessM... AssignedAccessManager Service

Running AudioEndpointBu... Windows Audio Endpoint Builder

Running Audiosrv Windows Audio

Stopped autotimesvc Cellular Time

Stopped AxInstSV ActiveX Installer (AxInstSV)

Stopped BcastDVRUserSer... GameDVR and Broadcast User Service\_...

Stopped BDESVC BitLocker Drive Encryption Service

Stopped BEService BattlEye Service

Running BFE Base Filtering Engine

Stopped BITS Background Intelligent Transfer Ser...

Stopped BluetoothUserSe... Bluetooth User Support Service\_265e...

Running BrokerInfrastru... Background Tasks Infrastructure Ser...

Running BTAGService Bluetooth Audio Gateway Service

Running BthAvctpSvc AVCTP service

Running bthserv Bluetooth Support Service

Running camsvc Capability Access Manager Service

Stopped CaptureService\_... CaptureService\_265e608d

Running cbdhsvc\_265e608d Clipboard User Service\_265e608d

Running CDPSvc Connected Devices Platform Service

Running CDPUserSvc\_265e... Connected Devices Platform User Ser...

Stopped CertPropSvc Certificate Propagation

Running ClickToRunSvc Microsoft Office Click-to-Run Service

Stopped ClipSVC Client License Service (ClipSVC)

Stopped cloudidsvc Microsoft Cloud Identity Service

Stopped COMSysApp COM+ System Application

Stopped ConsentUxUserSv... ConsentUX User Service\_265e608d

Running CoreMessagingRe... CoreMessaging

Running CorsairGamingAu... Corsair Gaming Audio Configuration ...

Running CorsairLLAService Corsair LLA Service

Running CorsairService Corsair Service

Stopped CredentialEnrol... CredentialEnrollmentManagerUserSvc\_...

Running CryptSvc Cryptographic Services

Stopped CscService Offline Files

Running DcomLaunch DCOM Server Process Launcher

Stopped defragsvc Optimize drives

Stopped DeviceAssociati... DeviceAssociationBroker\_265e608d

Running DeviceAssociati... Device Association Service

Running DeviceInstall Device Install Service

Stopped DevicePickerUse... DevicePicker\_265e608d

Running DevicesFlowUser... DevicesFlow\_265e608d

Stopped DevQueryBroker DevQuery Background Discovery Broker

Running Dhcp DHCP Client

Stopped diagnosticshub.... Microsoft (R) Diagnostics Hub Stand...

Stopped diagsvc Diagnostic Execution Service

Running DiagTrack Connected User Experiences and Tele...

Stopped DialogBlockingS... DialogBlockingService

Running DispBrokerDeskt... Display Policy Service

Running DisplayEnhancem... Display Enhancement Service

Stopped DmEnrollmentSvc Device Management Enrollment Service

Stopped dmwappushservice Device Management Wireless Applicat...

Running Dnscache DNS Client

Running DoSvc Delivery Optimization

Stopped dot3svc Wired AutoConfig

Running DPS Diagnostic Policy Service

Stopped DsmSvc Device Setup Manager

Running DsSvc Data Sharing Service

Running DusmSvc Data Usage

Stopped EapHost Extensible Authentication Protocol

Stopped EasyAntiCheat EasyAntiCheat

Stopped EasyAntiCheat\_EOS Easy Anti-Cheat (Epic Online Services)

Stopped edgeupdate Microsoft Edge Update Service (edge...

Stopped edgeupdatem Microsoft Edge Update Service (edge...

Running EFS Encrypting File System (EFS)

Stopped embeddedmode Embedded Mode

Stopped EntAppSvc Enterprise App Management Service

Running EventLog Windows Event Log

Running EventSystem COM+ Event System

Stopped Fax Fax

Stopped fdPHost Function Discovery Provider Host

Stopped FDResPub Function Discovery Resource Publica...

Stopped fhsvc File History Service

Stopped FileSyncHelper FileSyncHelper

Running FontCache Windows Font Cache Service

Stopped FrameServer Windows Camera Frame Server

Stopped FrameServerMonitor Windows Camera Frame Server Monitor

Running FvSvc NVIDIA FrameView SDK service

Running GamingServices Gaming Services

Running GamingServicesNet Gaming Services

Stopped GoogleChromeEle... Google Chrome Elevation Service (Go...

Stopped gpsvc Group Policy Client

Stopped GraphicsPerfSvc GraphicsPerfSvc

Stopped gupdate Google Update Service (gupdate)

Stopped gupdatem Google Update Service (gupdatem)

Running hidserv Human Interface Device Service

Running HvHost HV Host Service

Stopped icssvc Windows Mobile Hotspot Service

Running iCUEDevicePlugi... iCUE device plugin host service

Running IKEEXT IKE and AuthIP IPsec Keying Modules

Running InstallService Microsoft Store Install Service

Running iphlpsvc IP Helper

Stopped IpxlatCfgSvc IP Translation Configuration Service

Running KeyIso CNG Key Isolation

Stopped KtmRm KtmRm for Distributed Transaction C...

Running LanmanServer Server

Running LanmanWorkstation Workstation

Stopped lfsvc Geolocation Service

Running LGHUBUpdaterSer... LGHUB Updater Service

Running LicenseManager Windows License Manager Service

Stopped lltdsvc Link-Layer Topology Discovery Mapper

Running lmhosts TCP/IP NetBIOS Helper

Running LSM Local Session Manager

Stopped LxpSvc Language Experience Service

Stopped MapsBroker Downloaded Maps Manager

Stopped McpManagementSe... McpManagementService

Stopped MessagingServic... MessagingService\_265e608d

Stopped MicrosoftEdgeEl... Microsoft Edge Elevation Service (M...

Stopped MixedRealityOpe... Windows Mixed Reality OpenXR Service

Running mpssvc Windows Defender Firewall

Stopped MSDTC Distributed Transaction Coordinator

Stopped MSiSCSI Microsoft iSCSI Initiator Service

Stopped msiserver Windows Installer

Stopped MsKeyboardFilter Microsoft Keyboard Filter

Running NahimicService Nahimic service

Stopped NaturalAuthenti... Natural Authentication

Stopped NcaSvc Network Connectivity Assistant

Running NcbService Network Connection Broker

Stopped NcdAutoSetup Network Connected Devices Auto-Setup

Stopped Netlogon Netlogon

Stopped Netman Network Connections

Running netprofm Network List Service

Stopped NetSetupSvc Network Setup Service

Stopped NetTcpPortSharing Net.Tcp Port Sharing Service

Stopped NgcCtnrSvc Microsoft Passport Container

Stopped NgcSvc Microsoft Passport

Stopped NlaSvc Network Location Awareness

Running NordUpdaterService NordSec Update Service

Running nordvpn-service nordvpn-service

Running NPSMSvc\_265e608d NPSMSvc\_265e608d

Running nsi Network Store Interface Service

Running NvContainerLoca... NVIDIA LocalSystem Container

Running NVDisplay.Conta... NVIDIA Display Container LS

Stopped OneDrive Update... OneDrive Updater Service

Running OneSyncSvc\_265e... Sync Host\_265e608d

Stopped p2pimsvc Peer Networking Identity Manager

Stopped p2psvc Peer Networking Grouping

Stopped P9RdrService\_26... P9RdrService\_265e608d

Running PcaSvc Program Compatibility Assistant Ser...

Stopped PeerDistSvc BranchCache

Stopped PenService\_265e... PenService\_265e608d

Stopped perceptionsimul... Windows Perception Simulation Service

Stopped PerfHost Performance Counter DLL Host

Stopped PhoneSvc Phone Service

Running PimIndexMainten... Contact Data\_265e608d

Stopped pla Performance Logs & Alerts

Running PlugPlay Plug and Play

Stopped PNRPAutoReg PNRP Machine Name Publication Service

Stopped PNRPsvc Peer Name Resolution Protocol

Stopped PolicyAgent IPsec Policy Agent

Running Power Power

Stopped PrintNotify Printer Extensions and Notifications

Stopped PrintWorkflowUs... PrintWorkflow\_265e608d

Running ProfSvc User Profile Service

Stopped PushToInstall Windows PushToInstall Service

Running QWAVE Quality Windows Audio Video Experience

Stopped RasAuto Remote Access Auto Connection Manager

Running RasMan Remote Access Connection Manager

Stopped RemoteAccess Routing and Remote Access

Stopped RemoteRegistry Remote Registry

Stopped RetailDemo Retail Demo Service

Running RmSvc Radio Management Service

Running RpcEptMapper RPC Endpoint Mapper

Stopped RpcLocator Remote Procedure Call (RPC) Locator

Running RpcSs Remote Procedure Call (RPC)

Running SamSs Security Accounts Manager

Stopped SCardSvr Smart Card

Stopped ScDeviceEnum Smart Card Device Enumeration Service

Running Schedule Task Scheduler

Stopped SCPolicySvc Smart Card Removal Policy

Stopped SDRSVC Windows Backup

Stopped seclogon Secondary Logon

Running SecurityHealthS... Windows Security Service

Stopped SEMgrSvc Payments and NFC/SE Manager

Running SENS System Event Notification Service

Stopped Sense Windows Defender Advanced Threat Pr...

Stopped SensorDataService Sensor Data Service

Stopped SensorService Sensor Service

Stopped SensrSvc Sensor Monitoring Service

Stopped SessionEnv Remote Desktop Configuration

Running SgrmBroker System Guard Runtime Monitor Broker

Stopped SharedAccess Internet Connection Sharing (ICS)

Stopped SharedRealitySvc Spatial Data Service

Running ShellHWDetection Shell Hardware Detection

Stopped shpamsvc Shared PC Account Manager

Stopped smphost Microsoft Storage Spaces SMP

Stopped SmsRouter Microsoft Windows SMS Router Service.

Stopped SNMPTrap SNMP Trap

Stopped spectrum Windows Perception Service

Running Spooler Print Spooler

Stopped sppsvc Software Protection

Running SSDPSRV SSDP Discovery

Stopped ssh-agent OpenSSH Authentication Agent

Running SstpSvc Secure Socket Tunneling Protocol Se...

Running StateRepository State Repository Service

Stopped Steam Client Se... Steam Client Service

Stopped StiSvc Windows Image Acquisition (WIA)

Running StorSvc Storage Service

Stopped svsvc Spot Verifier

Stopped swprv Microsoft Software Shadow Copy Prov...

Running SysMain SysMain

Running SystemEventsBroker System Events Broker

Running TabletInputService Touch Keyboard and Handwriting Pane...

Stopped TapiSrv Telephony

Stopped TermService Remote Desktop Services

Running Themes Themes

Stopped TieringEngineSe... Storage Tiers Management

Running TimeBrokerSvc Time Broker

Running TokenBroker Web Account Manager

Running TrkWks Distributed Link Tracking Client

Stopped TroubleshootingSvc Recommended Troubleshooting Service

Stopped TrustedInstaller Windows Modules Installer

Stopped tzautoupdate Auto Time Zone Updater

Running UdkUserSvc\_265e... Udk User Service\_265e608d

Stopped UevAgentService User Experience Virtualization Service

Stopped uhssvc Microsoft Update Health Service

Stopped UmRdpService Remote Desktop Services UserMode Po...

Running UnistoreSvc\_265... User Data Storage\_265e608d

Stopped upnphost UPnP Device Host

Running UserDataSvc\_265... User Data Access\_265e608d

Running UserManager User Manager

Running UsoSvc Update Orchestrator Service

Stopped VacSvc Volumetric Audio Compositor Service

Running VaultSvc Credential Manager

Stopped VBoxSDS VirtualBox system service

Stopped vds Virtual Disk

Stopped vmicguestinterface Hyper-V Guest Service Interface

Stopped vmicheartbeat Hyper-V Heartbeat Service

Stopped vmickvpexchange Hyper-V Data Exchange Service

Stopped vmicrdv Hyper-V Remote Desktop Virtualizati...

Stopped vmicshutdown Hyper-V Guest Shutdown Service

Stopped vmictimesync Hyper-V Time Synchronization Service

Stopped vmicvmsession Hyper-V PowerShell Direct Service

Stopped vmicvss Hyper-V Volume Shadow Copy Requestor

Stopped VSS Volume Shadow Copy

Running W32Time Windows Time

Stopped WaaSMedicSvc Windows Update Medic Service

Stopped WalletService WalletService

Stopped WarpJITSvc Warp JIT Service

Stopped wbengine Block Level Backup Engine Service

Stopped WbioSrvc Windows Biometric Service

Running Wcmsvc Windows Connection Manager

Stopped wcncsvc Windows Connect Now - Config Registrar

Running WdiServiceHost Diagnostic Service Host

Stopped WdiSystemHost Diagnostic System Host

Running WdNisSvc Microsoft Defender Antivirus Networ...

Running WebClient WebClient

Stopped Wecsvc Windows Event Collector

Stopped WEPHOSTSVC Windows Encryption Provider Host Se...

Stopped wercplsupport Problem Reports Control Panel Support

Stopped WerSvc Windows Error Reporting Service

Stopped WFDSConMgrSvc Wi-Fi Direct Services Connection Ma...

Stopped WiaRpc Still Image Acquisition Events

Running WinDefend Microsoft Defender Antivirus Service

Running WinHttpAutoProx... WinHTTP Web Proxy Auto-Discovery Se...

Running Winmgmt Windows Management Instrumentation

Stopped WinRM Windows Remote Management (WS-Manag...

Stopped wisvc Windows Insider Service

Running WlanSvc WLAN AutoConfig

Stopped wlidsvc Microsoft Account Sign-in Assistant

Stopped wlpasvc Local Profile Assistant Service

Stopped WManSvc Windows Management Service

Stopped wmiApSrv WMI Performance Adapter

Stopped WMPNetworkSvc Windows Media Player Network Sharin...

Stopped workfolderssvc Work Folders

Stopped WpcMonSvc Parental Controls

Stopped WPDBusEnum Portable Device Enumerator Service

Running WpnService Windows Push Notifications System S...

Running WpnUserService\_... Windows Push Notifications User Ser...

Running wscsvc Security Center

Running WSearch Windows Search

Stopped wuauserv Windows Update

Stopped WwanSvc WWAN AutoConfig

Stopped XblAuthManager Xbox Live Auth Manager

Stopped XblGameSave Xbox Live Game Save

Running XboxGipSvc Xbox Accessory Management Service

Stopped XboxNetApiSvc Xbox Live Networking Service

PS C:\Users\Andrew>

<<<<< Paste your terminal capture above this line <<<<<

**Note: There is no quiz for this week.**

# Rubric:

**Part 2:**

Step 1-5: 6 points each

Must capture the actual terminal interactions, not just commands, to receive full credit.

**Part 3:**

Step 1-15: 2 points each