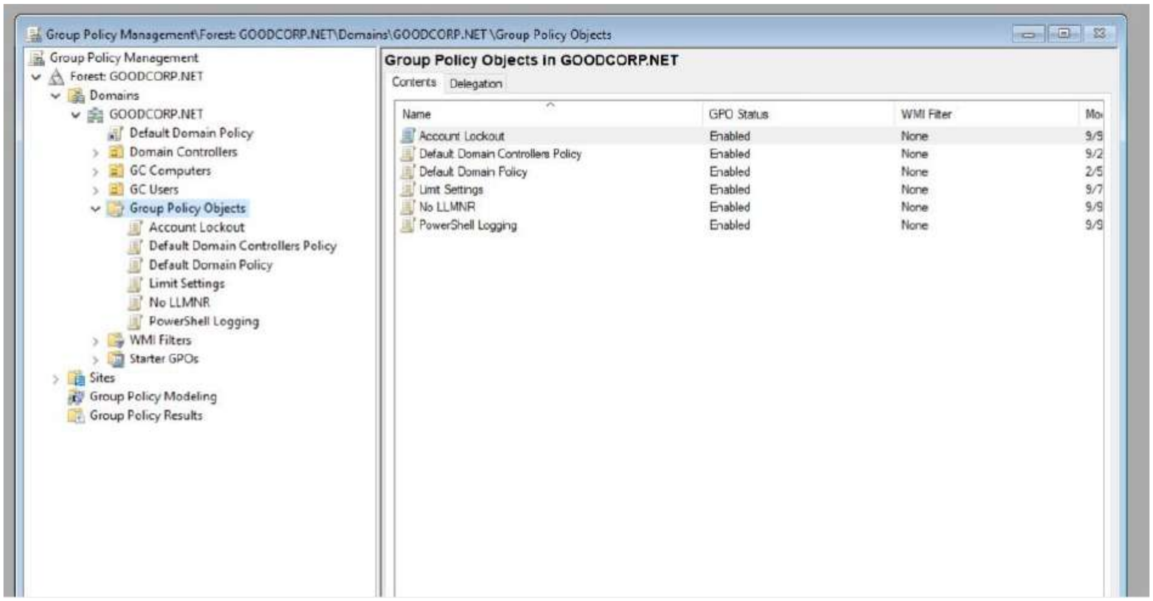
A Day in the Life of a Windows Sysadmin

This assignment built upon the Group Policy Objectives activities from the previous class, focusing on creating domain-hardening Group Policy Objects (GPOs) and revisiting PowerShell fundamentals.

I utilized the Windows Server machine and Windows 10 machine within the Azure Windows RDP Host machine as my lab environment. To access the nested virtual machines, I opened the Hyper-V Manager in the Windows RDP Host machine. Additionally, I familiarized myself with a list of common Windows issues provided in the module's documentation.

Task 1: Create a GPO - Disable Local Link Multicast Name Resolution (LLMNR)

In this task, I successfully investigated and mitigated a potential attack vector within a Windows domain by disabling LLMNR on my Windows 10 machine via the GC Computers OU. I created a Group Policy Object named "No LLMNR," disabling the "Turn Off Multicast Name Resolution" policy under Computer Configuration\Policies\Administrative Templates\Network\DNS Client. I linked the GPO to the GC Computers organizational unit.

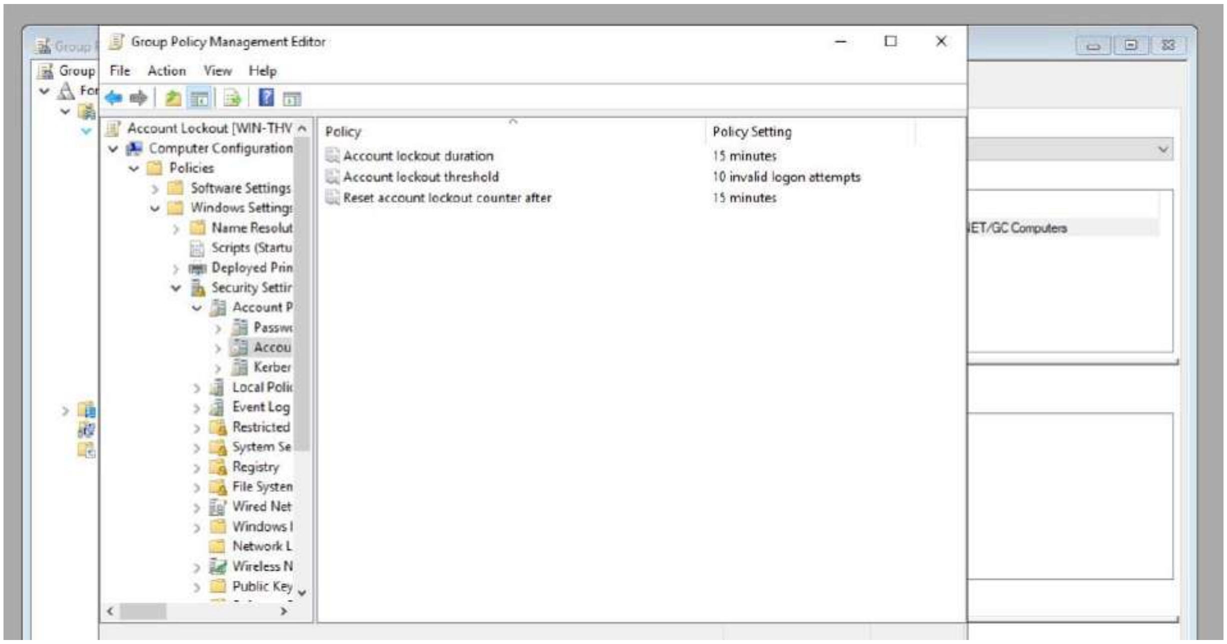


Group Policy Objects in GOODCORP.NET

Name	GPO Status	WMI Filter	Mo
Account Lockout	Enabled	None	9/9
Default Domain Controllers Policy	Enabled	None	9/2
Default Domain Policy	Enabled	None	2/5
Limit Settings	Enabled	None	9/7
No LLMNR	Enabled	None	9/9
PowerShell Logging	Enabled	None	9/9

Task 2: Create a GPO - Account Lockout

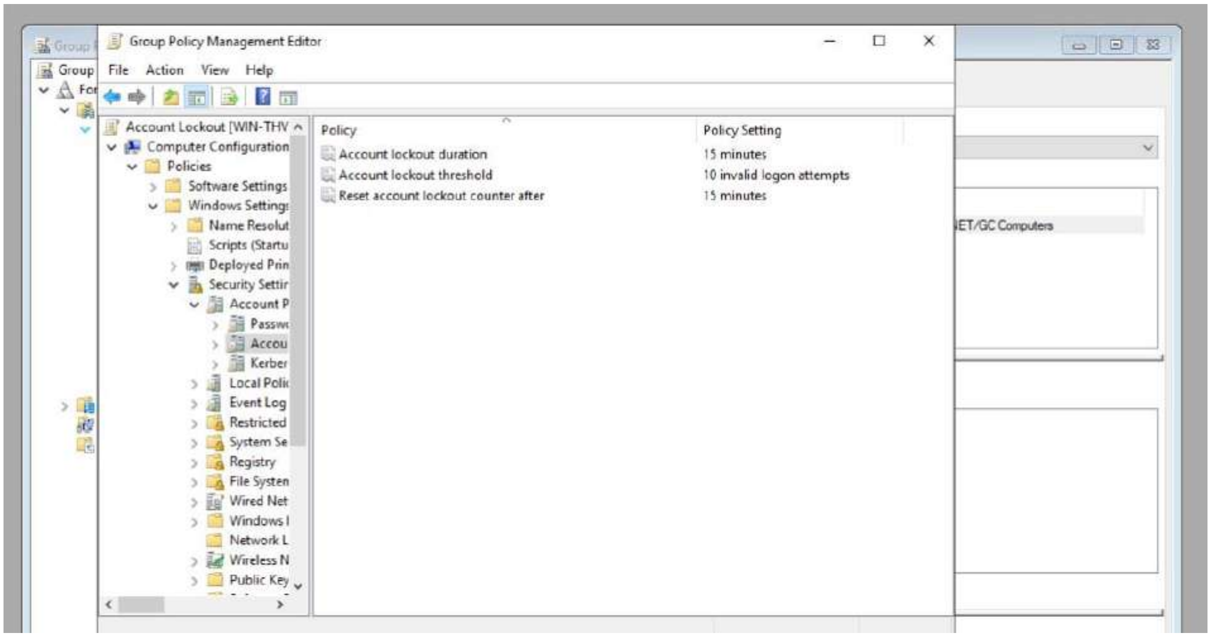
For security and compliance reasons, I implemented an account lockout policy on my Windows workstation. Following the Microsoft Security Guidance, I created a Group Policy Object named "Account Lockout" and configured a reasonable account lockout policy for the Windows 10 machine. I ensured that computer configuration policies applied to the GC Computers OU and linked the GPO accordingly.



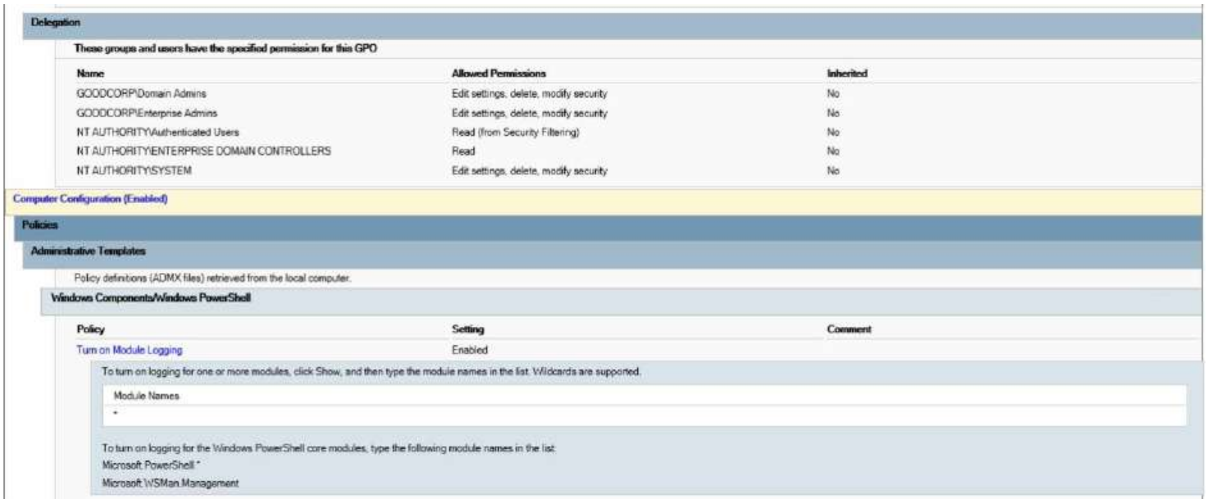
Policy	Policy Setting
Account lockout duration	15 minutes
Account lockout threshold	10 invalid logon attempts
Reset account lockout counter after	15 minutes

Task 3: Create a GPO - Enabling Verbose PowerShell Logging and Transcription

To enhance PowerShell logging and visibility, I created a Group Policy Object named "PowerShell Logging." This GPO combined multiple policies, including turning on module logging, PowerShell script block logging, script execution, and PowerShell transcription. I linked this GPO to the GC Computers OU, ensuring comprehensive logging for SIEM and forensic operations.



Policy	Policy Setting
Account lockout duration	15 minutes
Account lockout threshold	10 invalid logon attempts
Reset account lockout counter after	15 minutes



Delegation

These groups and users have the specified permission for this GPO

Name	Allowed Permissions	Inherited
GOODCORP\Domain Admins	Edit settings, delete, modify security	No
GOODCORP\Enterprise Admins	Edit settings, delete, modify security	No
NT AUTHORITY\Authenticated Users	Read (from Security Filtering)	No
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Read	No
NT AUTHORITY\SYSTEM	Edit settings, delete, modify security	No

Computer Configuration (Enabled)

Policies

Administrative Templates

Policy definitions (ADMX files) retrieved from the local computer.

Windows Components/Windows PowerShell

Policy	Setting	Comment
Turn on Module Logging	Enabled	

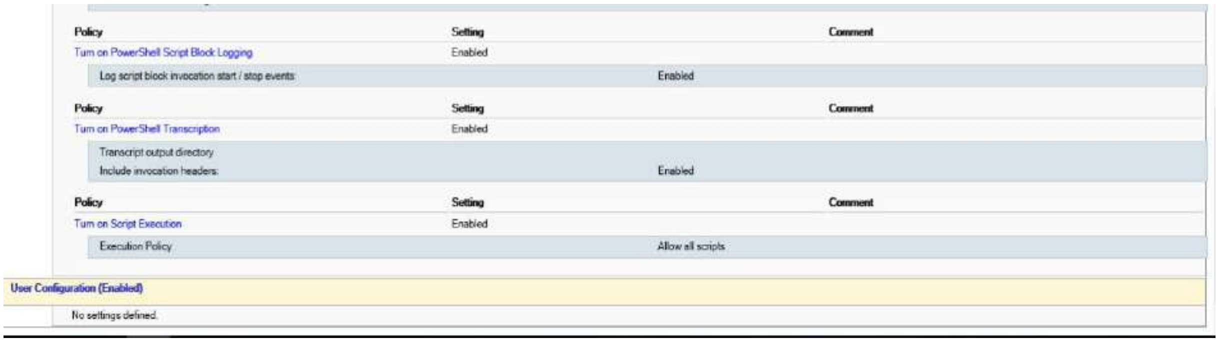
To turn on logging for one or more modules, click Show, and then type the module names in the list. Wildcards are supported.

Module Names
*

To turn on logging for the Windows PowerShell core modules, type the following module names in the list:

Microsoft.PowerShell.*

Microsoft.WSMan.Management



Policy	Setting	Comment
Turn on PowerShell Script Block Logging	Enabled	

Log script block invocation start / stop events:	Enabled

Policy	Setting	Comment
Turn on PowerShell Transcription	Enabled	

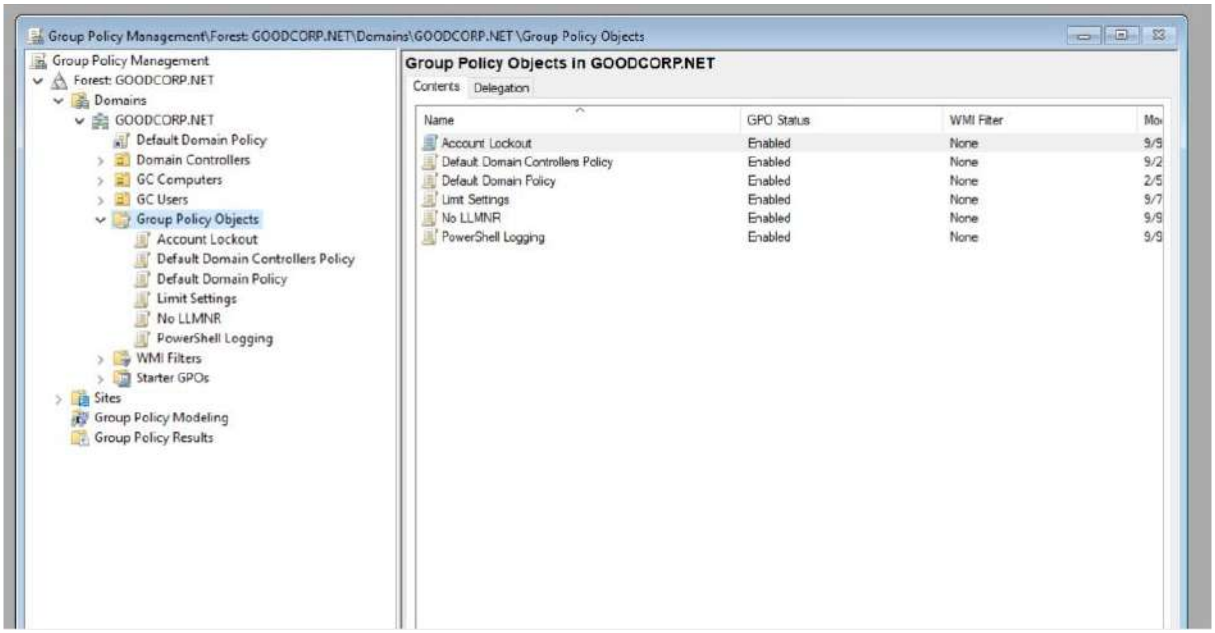
Transcript output directory	
Include invocation headers:	Enabled

Policy	Setting	Comment
Turn on Script Execution	Enabled	

Execution Policy	Allow all scripts

User Configuration (Enabled)

No settings defined.

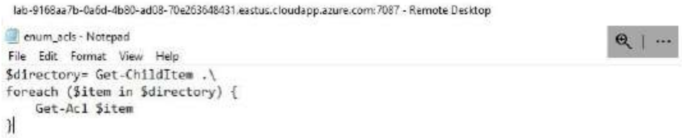


Group Policy Objects in GOODCORP.NET

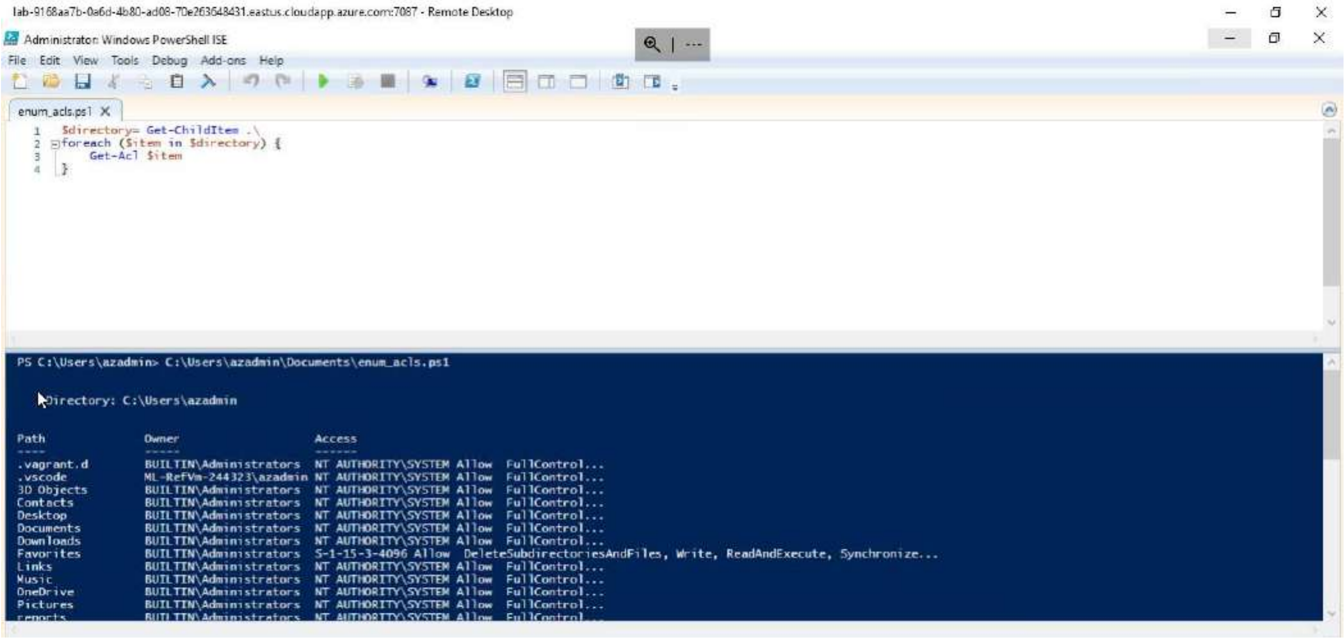
Name	GPO Status	WMI Filter	Mo
Account Lockout	Enabled	None	9/9
Default Domain Controllers Policy	Enabled	None	9/2
Default Domain Policy	Enabled	None	2/5
Limit Settings	Enabled	None	9/7
No LLMNR	Enabled	None	9/9
PowerShell Logging	Enabled	None	9/9

Task 4: Create a Script - Enumerate Access Control Lists

I successfully created a PowerShell script named "enum_acls.ps1" on my nested Windows 10 machine with the given credentials. This script enumerated the Access Control List of each file or subdirectory within the current working directory using the Get-Acl PowerShell cmdlet.


lab-9168aa7b-0a6d-4b80-ad08-70e263648431.eastus.cloudapp.azure.com:7087 - Remote Desktop
enum_acls - Notepad
File Edit Format View Help

```
$directory= Get-ChildItem .\
foreach ($item in $directory) {
    Get-Acl $item
}
```

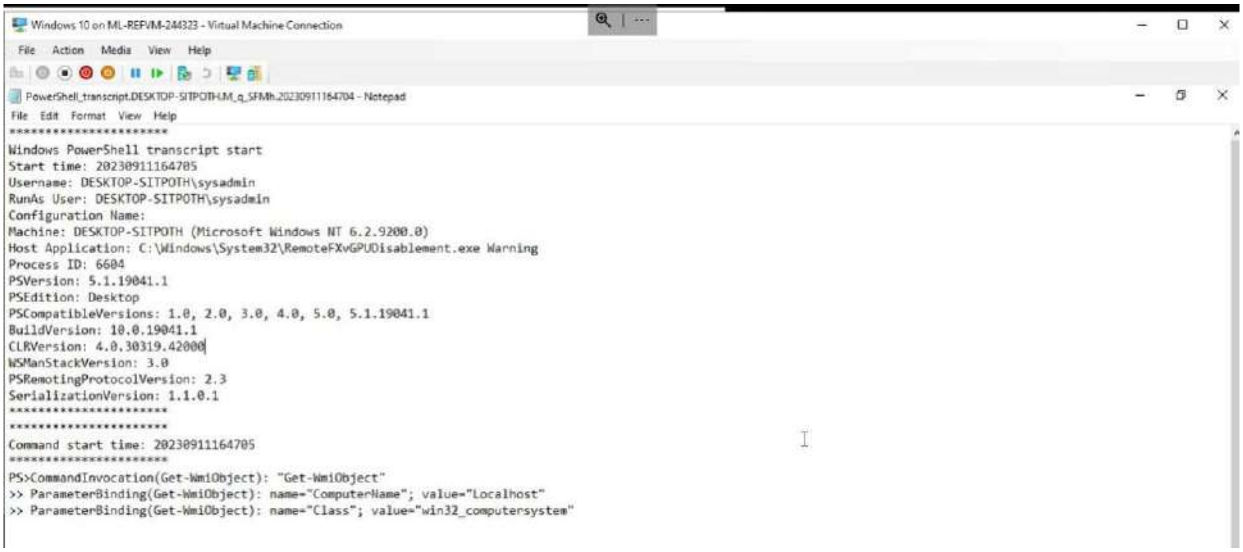

lab-9168aa7b-0a6d-4b80-ad08-70e263648431.eastus.cloudapp.azure.com:7087 - Remote Desktop
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
enum_acls.ps1

```
$directory= Get-ChildItem .\
foreach ($item in $directory) {
    Get-Acl $item
}
```

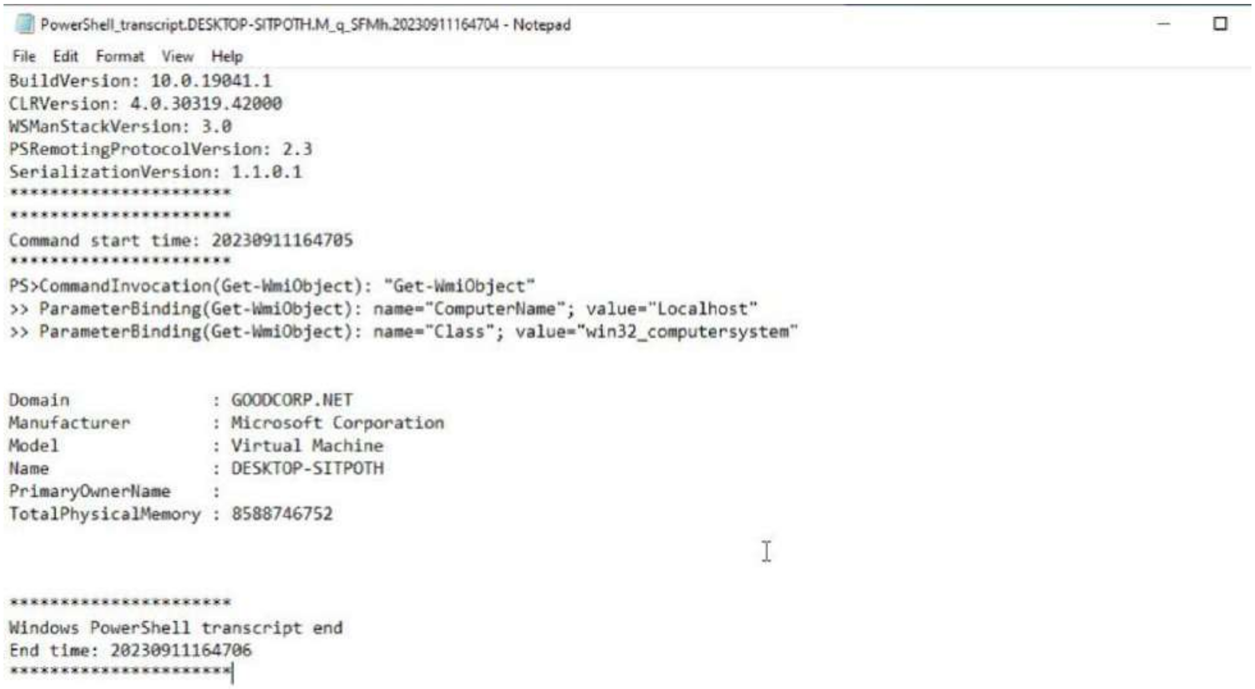
```
PS C:\Users\azadmin> C:\Users\azadmin\Documents\enum_acls.ps1


    Directory: C:\Users\azadmin


Path              Owner                      Access
----              -----                      ------
.vagrant.d        BUILTIN\Administrators     NT AUTHORITY\SYSTEM Allow  FullControl...
.vscode           ML-RefVm-244323\azadmin    NT AUTHORITY\SYSTEM Allow  FullControl...
3D Objects        BUILTIN\Administrators     NT AUTHORITY\SYSTEM Allow  FullControl...
Contacts          BUILTIN\Administrators     NT AUTHORITY\SYSTEM Allow  FullControl...
Desktop           BUILTIN\Administrators     NT AUTHORITY\SYSTEM Allow  FullControl...
Documents         BUILTIN\Administrators     NT AUTHORITY\SYSTEM Allow  FullControl...
Downloads         BUILTIN\Administrators     NT AUTHORITY\SYSTEM Allow  FullControl...
Favorites         BUILTIN\Administrators     S-1-15-3-4096 Allow  DeleteSubdirectoriesAndFiles, Write, ReadAndExecute, Synchronize...
Links             BUILTIN\Administrators     NT AUTHORITY\SYSTEM Allow  FullControl...
Music             BUILTIN\Administrators     NT AUTHORITY\SYSTEM Allow  FullControl...
OneDrive          BUILTIN\Administrators     NT AUTHORITY\SYSTEM Allow  FullControl...
Pictures          BUILTIN\Administrators     NT AUTHORITY\SYSTEM Allow  FullControl...
reports           BUILTIN\Administrators     NT AUTHORITY\SYSTEM Allow  FullControl...
```

Task 5: Verify Your PowerShell Logging GPO

I tested and verified the functionality of my PowerShell logging GPO. After running `gpupdate` in an administrative PowerShell window and relaunching PowerShell, I navigated to C:\Windows, ran the "enum_acls.ps1" script, and checked the C:\Users\sysadmin\Documents directory for the transcribed PowerShell logs, confirming that the GPO was working properly.

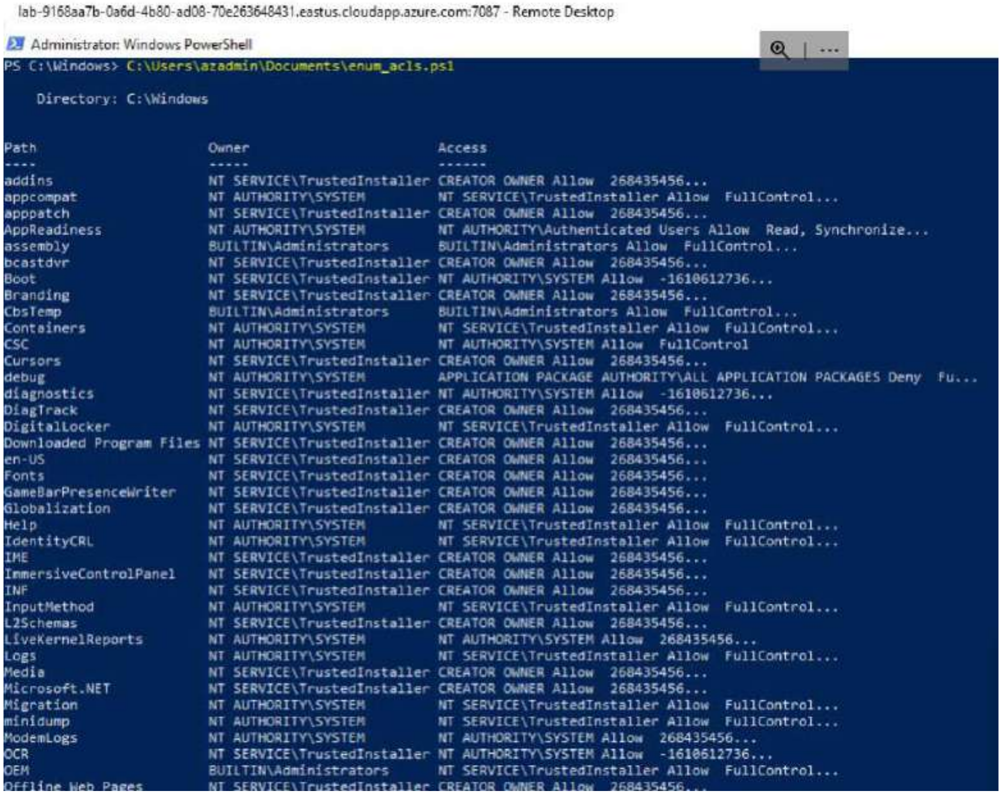

Windows 10 on ML-REFVM-244323 - Virtual Machine Connection
File Action Media View Help
PowerShell_transcript.DESKTOP-SITPOTH.M_q_SFMh.20230911164704 - Notepad
File Edit Format View Help

```
**********************
Windows PowerShell transcript start
Start time: 20230911164705
Username: DESKTOP-SITPOTH\sysadmin
RunAs User: DESKTOP-SITPOTH\sysadmin
Configuration Name:
Machine: DESKTOP-SITPOTH (Microsoft Windows NT 6.2.9200.0)
Host Application: C:\Windows\System32\RemoteFXvGPUDisablement.exe Warning
Process ID: 6604
PSVersion: 5.1.19041.1
PSEdition: Desktop
PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.19041.1
BuildVersion: 10.0.19041.1
CLRVersion: 4.0.30319.42000
WSManStackVersion: 3.0
PSRemotingProtocolVersion: 2.3
SerializationVersion: 1.1.0.1
**********************
**********************
Command start time: 20230911164705
**********************
PS>CommandInvocation(Get-WmiObject): "Get-WmiObject"
>> ParameterBinding(Get-WmiObject): name="ComputerName"; value="Localhost"
>> ParameterBinding(Get-WmiObject): name="Class"; value="win32_computersystem"
```



PowerShell_transcript.DESKTOP-SITPOTH.M_q_SFMh.20230911164704 - Notepad

```
BuildVersion: 10.0.19041.1
CLRVersion: 4.0.30319.42000
WSManStackVersion: 3.0
PSRemotingProtocolVersion: 2.3
SerializationVersion: 1.1.0.1
**********************
**********************
Command start time: 20230911164705
**********************
PS>CommandInvocation(Get-WmiObject): "Get-WmiObject"
>> ParameterBinding(Get-WmiObject): name="ComputerName"; value="Localhost"
>> ParameterBinding(Get-WmiObject): name="Class"; value="win32_computersystem"


Domain              : GOODCORP.NET
Manufacturer        : Microsoft Corporation
Model               : Virtual Machine
Name                : DESKTOP-SITPOTH
PrimaryOwnerName    :
TotalPhysicalMemory : 8588746752



**********************
Windows PowerShell transcript end
End time: 20230911164706
**********************
```



lab-9168aa7b-0a6d-4b80-ad08-70e263648431.eastus.cloudapp.azure.com:7087 - Remote Desktop

Administrator: Windows PowerShell

```
PS C:\Windows> C:\Users\azadmin\Documents\enum_acls.ps1

    Directory: C:\Windows


Path                     Owner                       Access
----                     -----                       ------
addins                   NT SERVICE\TrustedInstaller CREATOR OWNER Allow  268435456...
appcompat                NT AUTHORITY\SYSTEM         NT SERVICE\TrustedInstaller Allow  FullControl...
apppatch                 NT SERVICE\TrustedInstaller CREATOR OWNER Allow  268435456...
AppReadiness             NT AUTHORITY\SYSTEM         NT AUTHORITY\Authenticated Users Allow  Read, Synchronize...
assembly                 BUILTIN\Administrators      BUILTIN\Administrators Allow  FullControl...
bcastdvr                 NT SERVICE\TrustedInstaller CREATOR OWNER Allow  268435456...
Boot                     NT SERVICE\TrustedInstaller NT AUTHORITY\SYSTEM Allow  -1610612736...
Branding                 NT SERVICE\TrustedInstaller CREATOR OWNER Allow  268435456...
CbsTemp                  BUILTIN\Administrators      BUILTIN\Administrators Allow  FullControl...
Containers               NT AUTHORITY\SYSTEM         NT SERVICE\TrustedInstaller Allow  FullControl...
CSC                      NT AUTHORITY\SYSTEM         NT AUTHORITY\SYSTEM Allow  FullControl
Cursors                  NT SERVICE\TrustedInstaller CREATOR OWNER Allow  268435456...
debug                    NT AUTHORITY\SYSTEM         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Deny  Fu...
diagnostics              NT SERVICE\TrustedInstaller NT AUTHORITY\SYSTEM Allow  -1610612736...
DiagTrack                NT SERVICE\TrustedInstaller CREATOR OWNER Allow  268435456...
DigitalLocker            NT AUTHORITY\SYSTEM         NT SERVICE\TrustedInstaller Allow  FullControl...
Downloaded Program Files NT SERVICE\TrustedInstaller CREATOR OWNER Allow  268435456...
en-US                    NT SERVICE\TrustedInstaller CREATOR OWNER Allow  268435456...
Fonts                    NT SERVICE\TrustedInstaller CREATOR OWNER Allow  268435456...
GameBarPresenceWriter    NT SERVICE\TrustedInstaller CREATOR OWNER Allow  268435456...
Globalization            NT SERVICE\TrustedInstaller CREATOR OWNER Allow  268435456...
Help                     NT AUTHORITY\SYSTEM         NT SERVICE\TrustedInstaller Allow  FullControl...
IdentityCRL              NT AUTHORITY\SYSTEM         NT SERVICE\TrustedInstaller Allow  FullControl...
IME                      NT SERVICE\TrustedInstaller CREATOR OWNER Allow  268435456...
ImmersiveControlPanel    NT SERVICE\TrustedInstaller CREATOR OWNER Allow  268435456...
INF                      NT SERVICE\TrustedInstaller CREATOR OWNER Allow  268435456...
InputMethod              NT AUTHORITY\SYSTEM         NT SERVICE\TrustedInstaller Allow  FullControl...
L2Schemas                NT SERVICE\TrustedInstaller CREATOR OWNER Allow  268435456...
LiveKernelReports        NT AUTHORITY\SYSTEM         NT AUTHORITY\SYSTEM Allow  268435456...
Logs                     NT AUTHORITY\SYSTEM         NT SERVICE\TrustedInstaller Allow  FullControl...
Media                    NT SERVICE\TrustedInstaller CREATOR OWNER Allow  268435456...
Microsoft.NET            NT SERVICE\TrustedInstaller CREATOR OWNER Allow  268435456...
Migration                NT AUTHORITY\SYSTEM         NT SERVICE\TrustedInstaller Allow  FullControl...
minidump                 NT AUTHORITY\SYSTEM         NT SERVICE\TrustedInstaller Allow  FullControl...
ModemLogs                NT AUTHORITY\SYSTEM         NT AUTHORITY\SYSTEM Allow  268435456...
OCR                      NT SERVICE\TrustedInstaller NT AUTHORITY\SYSTEM Allow  -1610612736...
OEM                      BUILTIN\Administrators      NT SERVICE\TrustedInstaller Allow  FullControl...
Offline Web Pages        NT SERVICE\TrustedInstaller CREATOR OWNER Allow  268435456...
```