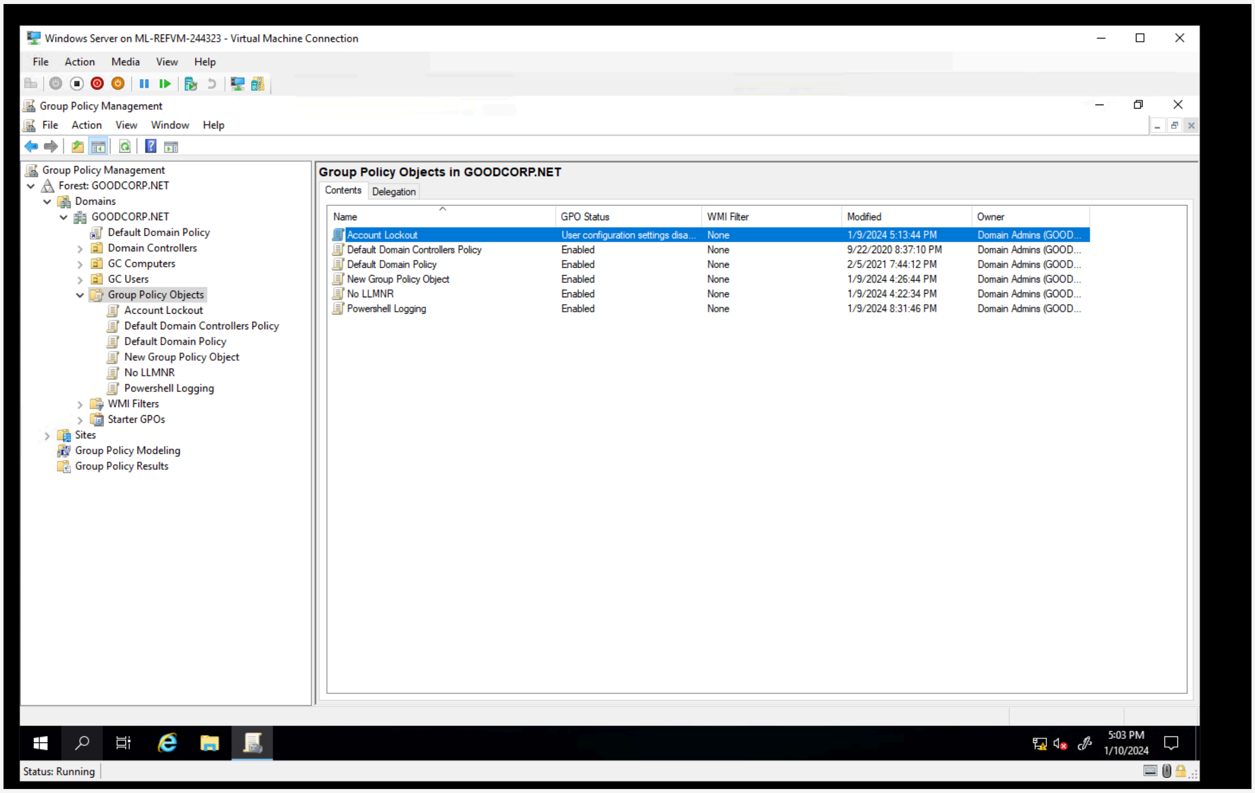
Cybersecurity

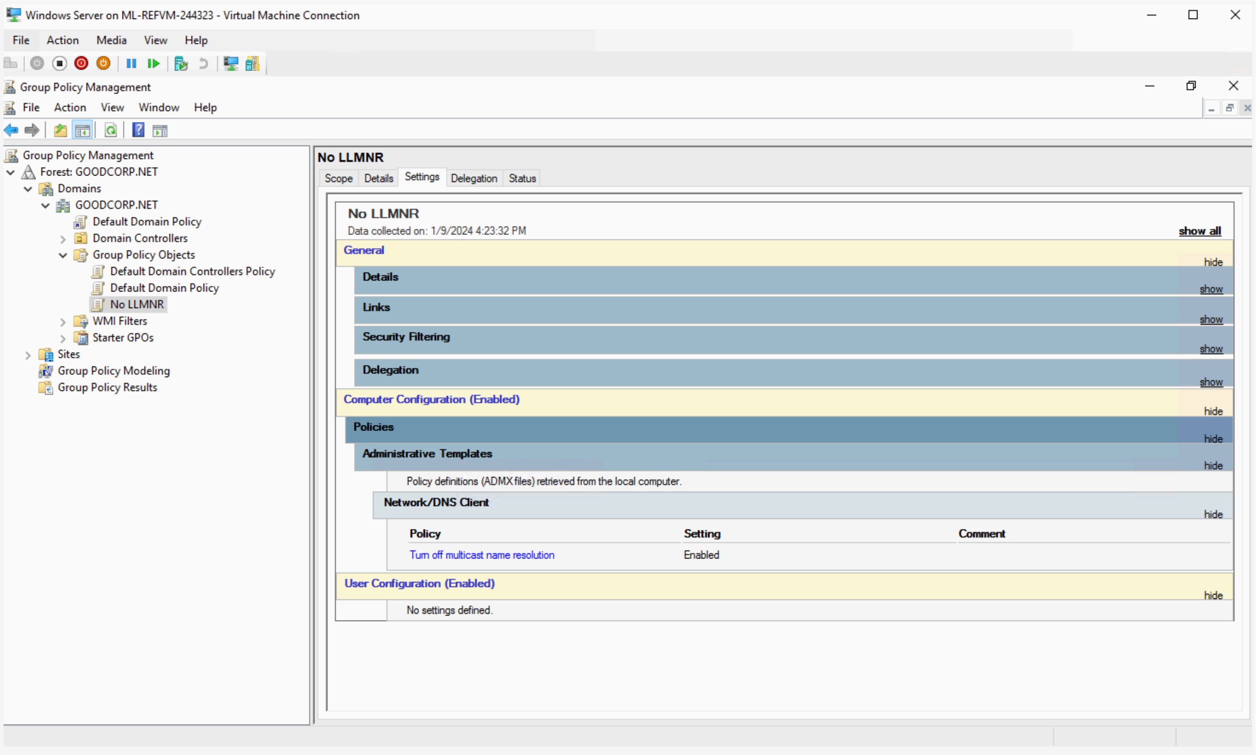
Module 7 A Day in the Life of a Windows Sysadmin

Deliverable for Task 1: A screenshot of all the GPOs created for this assignment. To find these, launch the Group Policy Management tool, select **Group Policy Objects**, and take a screenshot of the GPOs you've created. Name the screenshot file `GPOs`



Group Policy Objects in GOODCORP.NET

Name	GPO Status	WMI Filter	Modified	Owner
Account Lockout	User configuration settings disa...	None	1/9/2024 5:13:44 PM	Domain Admins (GOOD...
Default Domain Controllers Policy	Enabled	None	9/22/2020 8:37:10 PM	Domain Admins (GOOD...
Default Domain Policy	Enabled	None	2/5/2021 7:44:12 PM	Domain Admins (GOOD...
New Group Policy Object	Enabled	None	1/9/2024 4:26:44 PM	Domain Admins (GOOD...
No LLMNR	Enabled	None	1/9/2024 4:22:34 PM	Domain Admins (GOOD...
Powershell Logging	Enabled	None	1/9/2024 8:31:46 PM	Domain Admins (GOOD...



No LLMNR

No LLMNR

Data collected on: 1/9/2024 4:23:32 PM

General

Details

Links

Security Filtering

Delegation

Computer Configuration (Enabled)

Policies

Administrative Templates

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

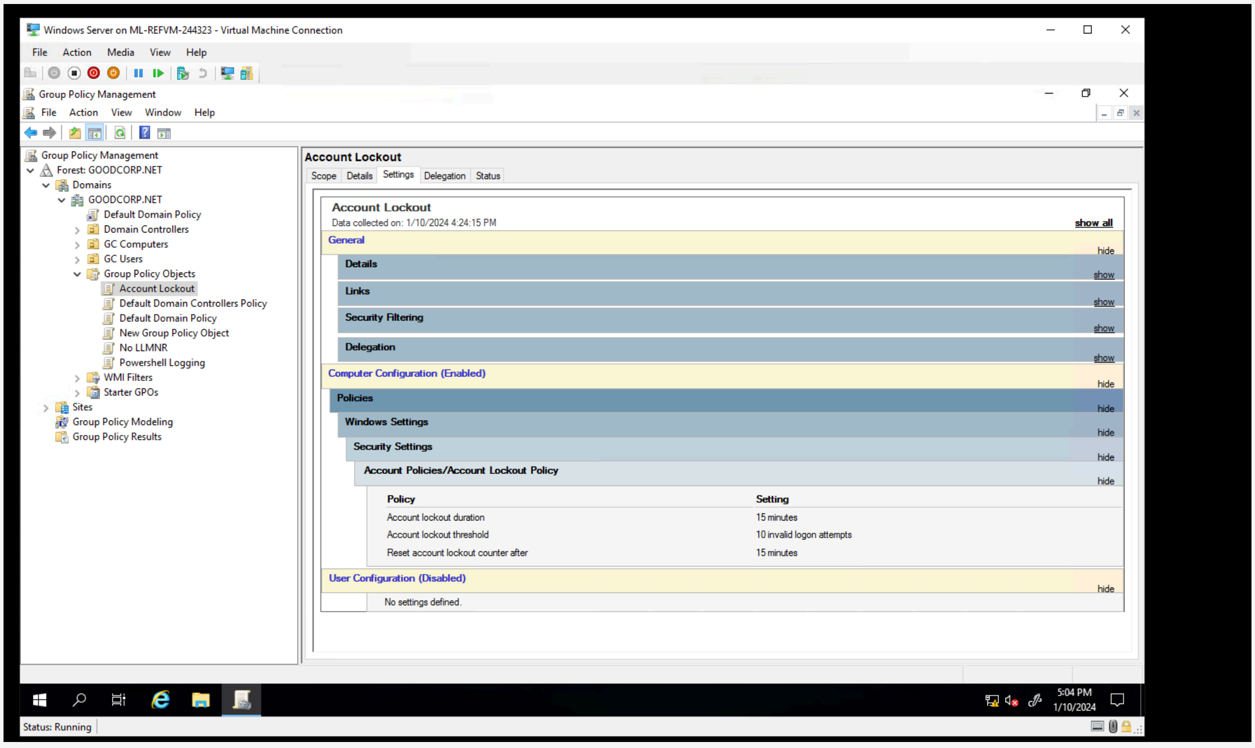
Network/DNS Client

Policy	Setting	Comment
Turn off multicast name resolution	Enabled	

User Configuration (Enabled)

No settings defined.

- **Deliverable for Task 2:** A screenshot of the different `Account Lockout` policies in Group Policy Management Editor. It should show the three values you set under the Policy and Policy Setting columns. Name the screenshot file `Account-Lockout-Policies`.



Account Lockout

Account Lockout

Data collected on: 1/10/2024 4:24:15 PM

General

Details

Links

Security Filtering

Delegation

Computer Configuration (Enabled)

Policies

Windows Settings

Security Settings

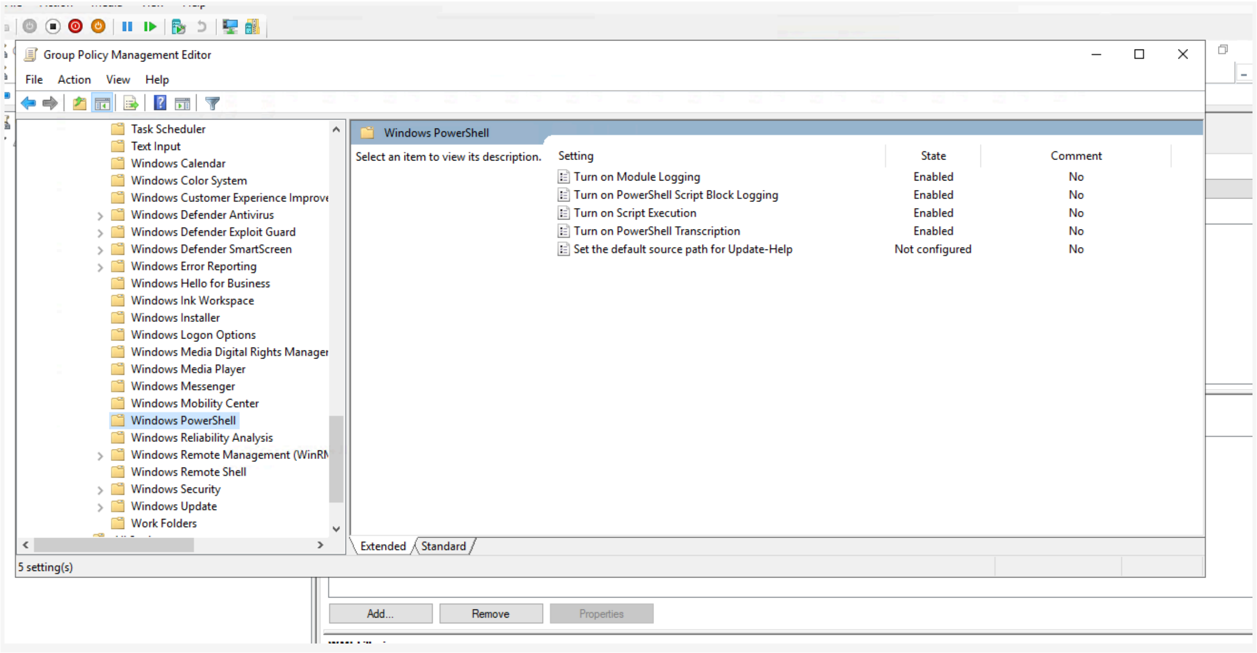
Account Policies/Account Lockout Policy

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

User Configuration (Disabled)

No settings defined.

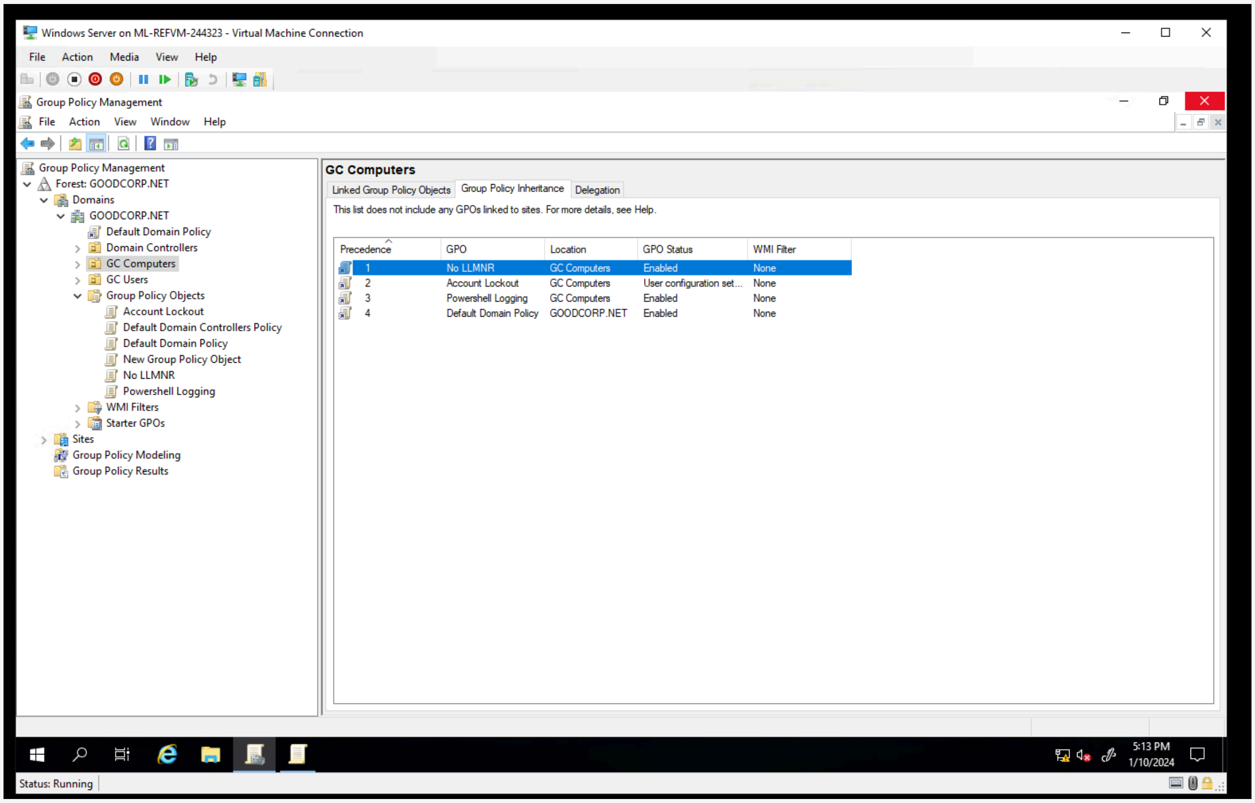
- **Deliverable for Task 3:** A screenshot of the different `Windows PowerShell` policies within the Group Policy Management Editor. Four of these should be enabled. Name the screenshot file `Windows-PowerShell-Policies`.



Select an item to view its description.

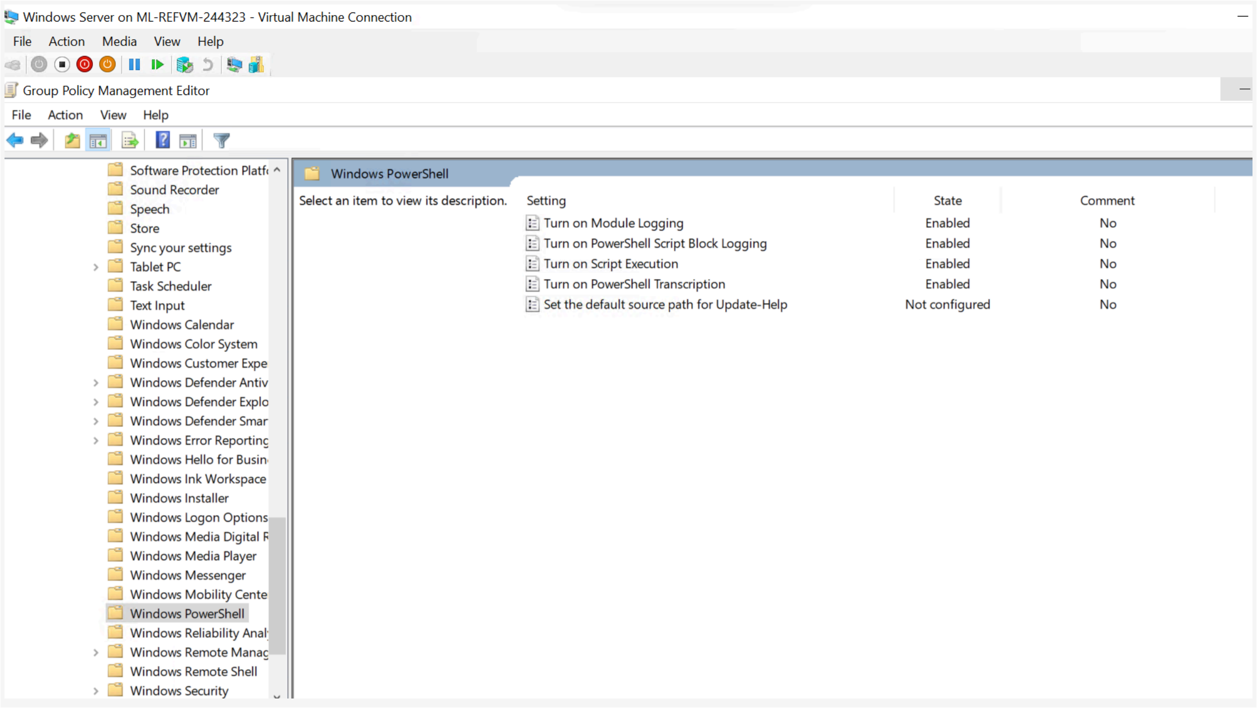
Setting	State	Comment
Turn on Module Logging	Enabled	No
Turn on PowerShell Script Block Logging	Enabled	No
Turn on Script Execution	Enabled	No
Turn on PowerShell Transcription	Enabled	No
Set the default source path for Update-Help	Not configured	No

5 setting(s)



This list does not include any GPOs linked to sites. For more details, see Help.

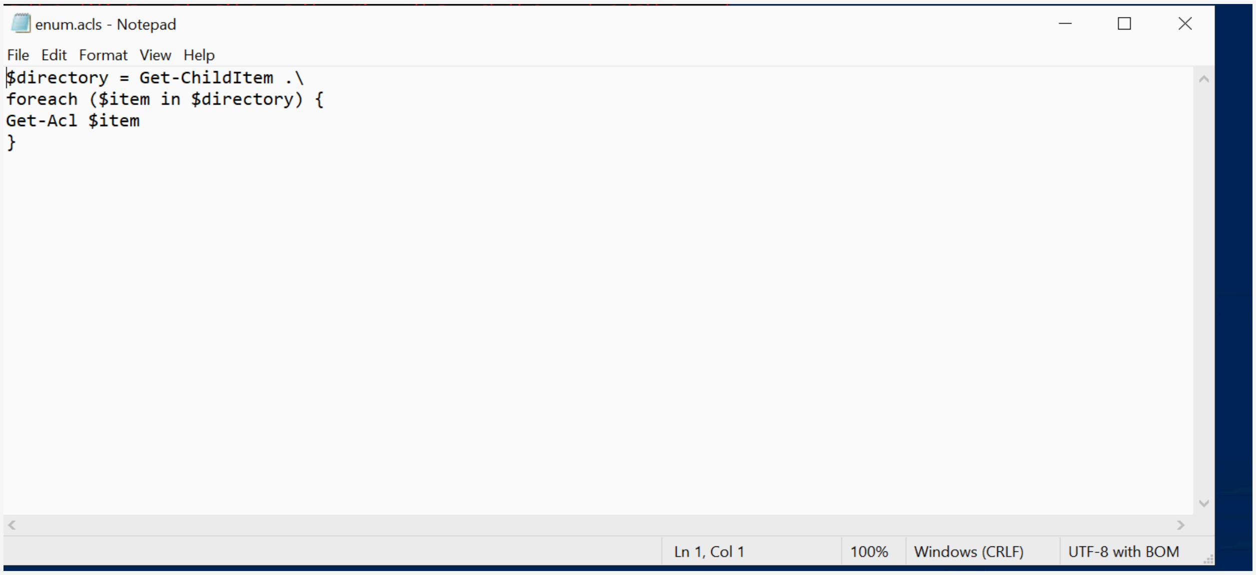
Precedence	GPO	Location	GPO Status	WMI Filter
1	No LLMNR	GC Computers	Enabled	None
2	Account Lockout	GC Computers	User configuration set...	None
3	Powershell Logging	GC Computers	Enabled	None
4	Default Domain Policy	GOODCORP.NET	Enabled	None



Select an item to view its description.

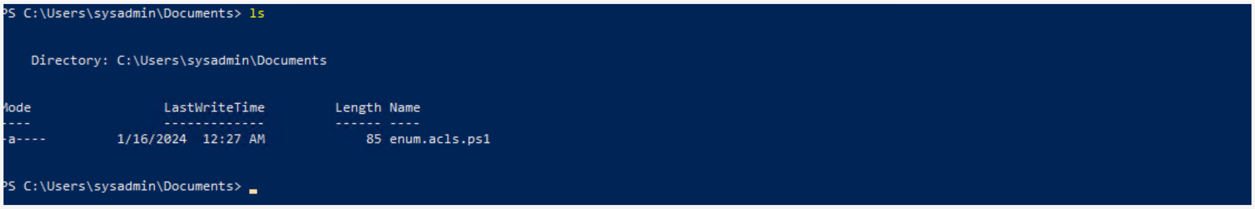
Setting	State	Comment
Turn on Module Logging	Enabled	No
Turn on PowerShell Script Block Logging	Enabled	No
Turn on Script Execution	Enabled	No
Turn on PowerShell Transcription	Enabled	No
Set the default source path for Update-Help	Not configured	No

- **Deliverable for Task 4:** A copy of your `enum_acls.ps1` script.



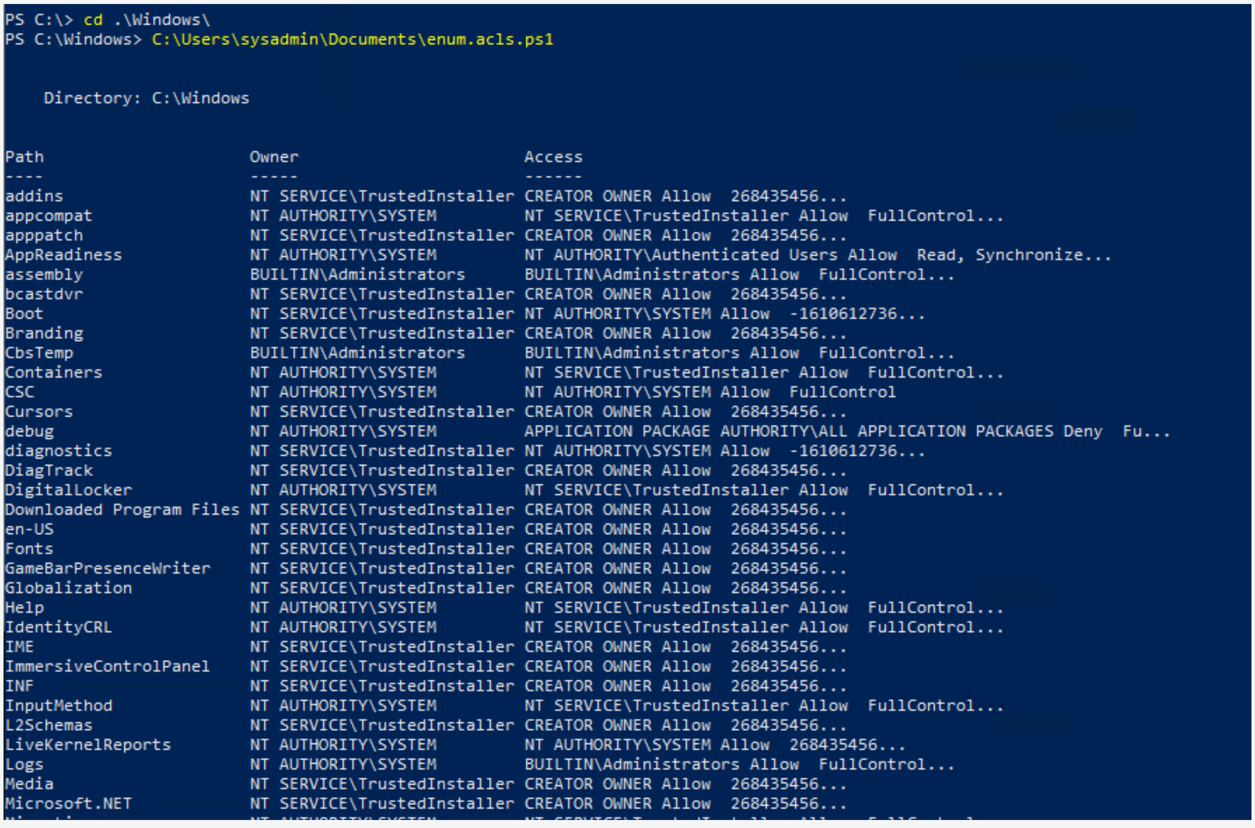
```
$directory = Get-ChildItem .\
foreach ($item in $directory) {
Get-Acl $item
}
```

-

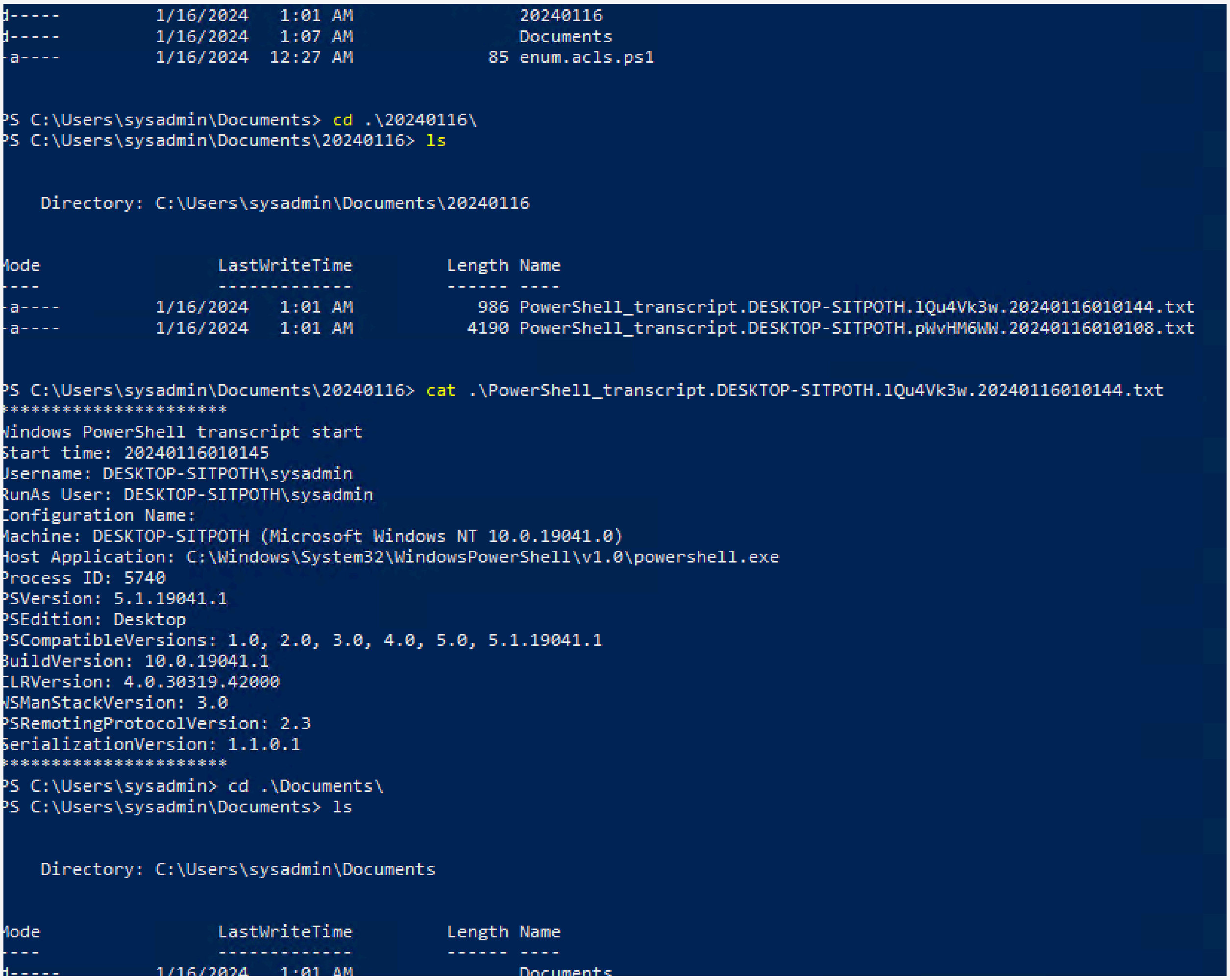


```
PS C:\Users\sysadmin\Documents> ls


    Directory: C:\Users\sysadmin\Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         1/16/2024  12:27 AM             85 enum.acls.ps1


PS C:\Users\sysadmin\Documents>
```

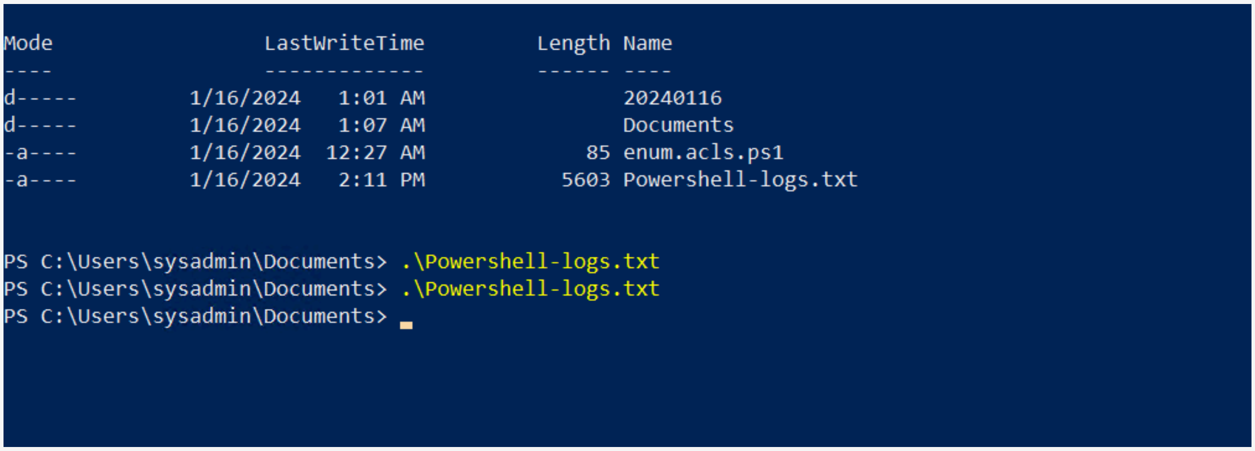
-



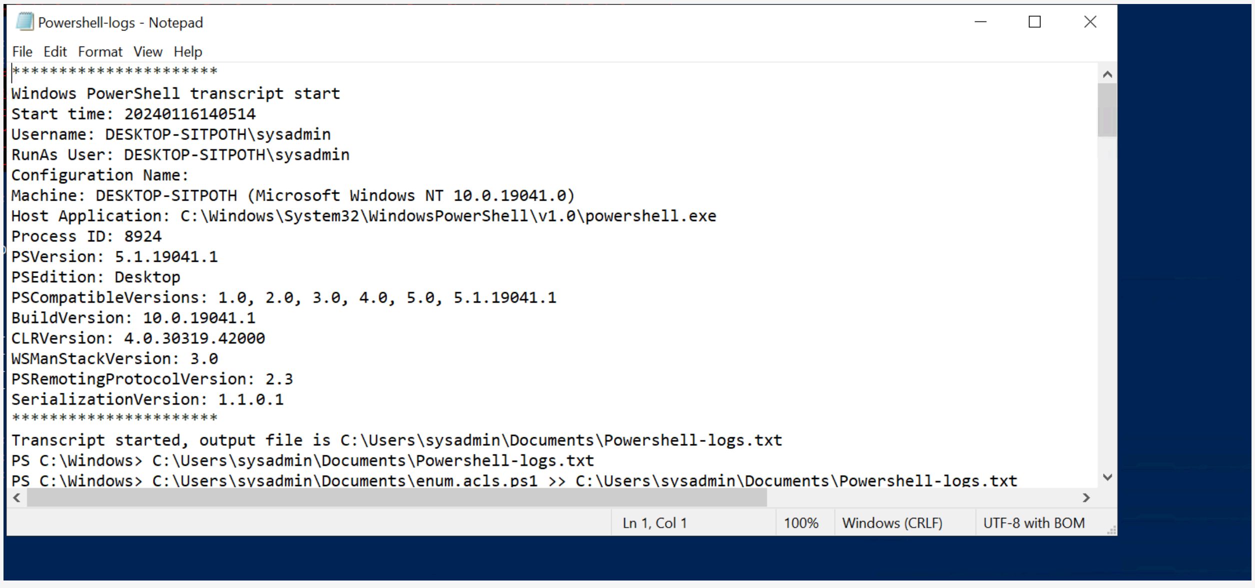
```
PS C:\> cd .\Windows\
PS C:\Windows> C:\Users\sysadmin\Documents\enum.acls.ps1


    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         BUILTIN\Administrators Allow  FullControl...
Media                    NT SERVICE\TrustedInstaller CREATOR OWNER Allow  268435456...
Microsoft.NET            NT SERVICE\TrustedInstaller CREATOR OWNER Allow  268435456...
```



```
d-----         1/16/2024   1:01 AM                20240116
d-----         1/16/2024   1:07 AM                Documents
-a----         1/16/2024  12:27 AM             85 enum.acls.ps1


PS C:\Users\sysadmin\Documents> cd .\20240116\
PS C:\Users\sysadmin\Documents\20240116> ls


    Directory: C:\Users\sysadmin\Documents\20240116


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         1/16/2024   1:01 AM            986 PowerShell_transcript.DESKTOP-SITPOTH.lQu4Vk3w.20240116010144.txt
-a----         1/16/2024   1:01 AM           4190 PowerShell_transcript.DESKTOP-SITPOTH.pWvHM6WW.20240116010108.txt


PS C:\Users\sysadmin\Documents\20240116> cat .\PowerShell_transcript.DESKTOP-SITPOTH.lQu4Vk3w.20240116010144.txt
**********************
Windows PowerShell transcript start
Start time: 20240116010145
Username: DESKTOP-SITPOTH\sysadmin
RunAs User: DESKTOP-SITPOTH\sysadmin
Configuration Name:
Machine: DESKTOP-SITPOTH (Microsoft Windows NT 10.0.19041.0)
Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Process ID: 5740
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
**********************
PS C:\Users\sysadmin> cd .\Documents\
PS C:\Users\sysadmin\Documents> ls


    Directory: C:\Users\sysadmin\Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         1/16/2024   1:01 AM                Documents
```



```
Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         1/16/2024   1:01 AM                20240116
d-----         1/16/2024   1:07 AM                Documents
-a----         1/16/2024  12:27 AM             85 enum.acls.ps1
-a----         1/16/2024   2:11 PM           5603 Powershell-logs.txt


PS C:\Users\sysadmin\Documents> .\Powershell-logs.txt
PS C:\Users\sysadmin\Documents> .\Powershell-logs.txt
PS C:\Users\sysadmin\Documents> _
```



```
**********************
Windows PowerShell transcript start
Start time: 20240116140514
Username: DESKTOP-SITPOTH\sysadmin
RunAs User: DESKTOP-SITPOTH\sysadmin
Configuration Name:
Machine: DESKTOP-SITPOTH (Microsoft Windows NT 10.0.19041.0)
Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Process ID: 8924
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
**********************
Transcript started, output file is C:\Users\sysadmin\Documents\Powershell-logs.txt
PS C:\Windows> C:\Users\sysadmin\Documents\Powershell-logs.txt
PS C:\Windows> C:\Users\sysadmin\Documents\enum.acls.ps1 >> C:\Users\sysadmin\Documents\Powershell-logs.txt
```