

Windows 10 VM

## Deliverable for Task 1:

### GPO's:

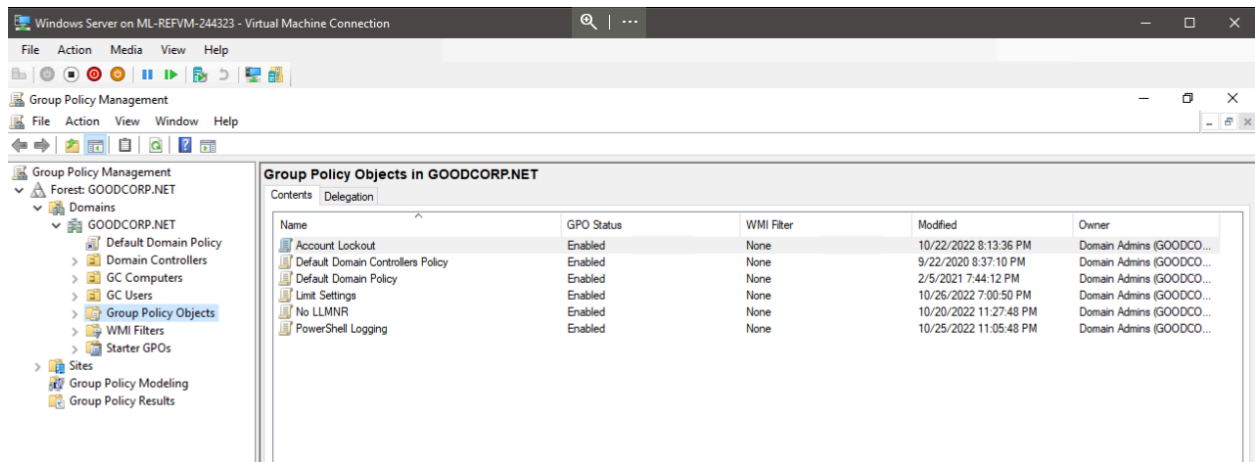


Figure 1.

## Deliverable for Task 2:

### Account-Lockout-Policies:

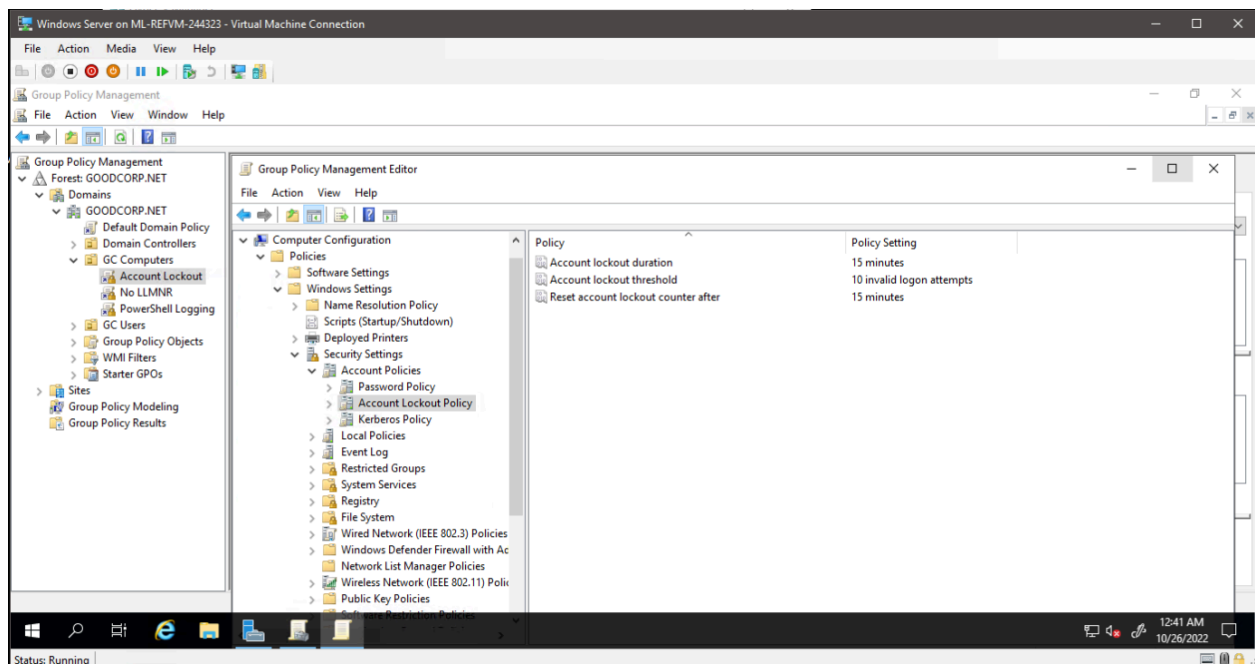


Figure 2.

## Deliverable for Task 3:

### Windows-PowerShell-Policies:

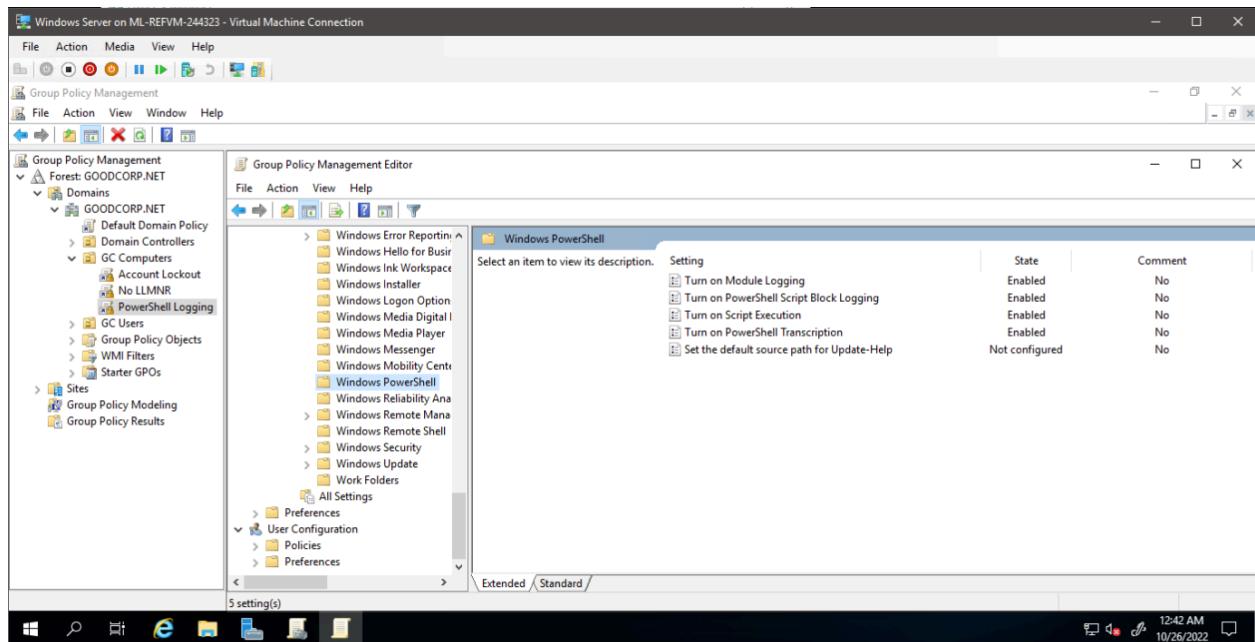


Figure 3.

## Deliverable for Task 4:

### Enum\_acls.ps1:

```
Administrator: Windows PowerShell

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

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

        Directory: C:\Users\sysadmin\Documents

Mode                LastWriteTime         Length Name
----                -
d-----          10/25/2022 11:28 PM             20221025
-a----          10/25/2022 10:39 PM             85 enum_acls.ps1

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

Figure 4.

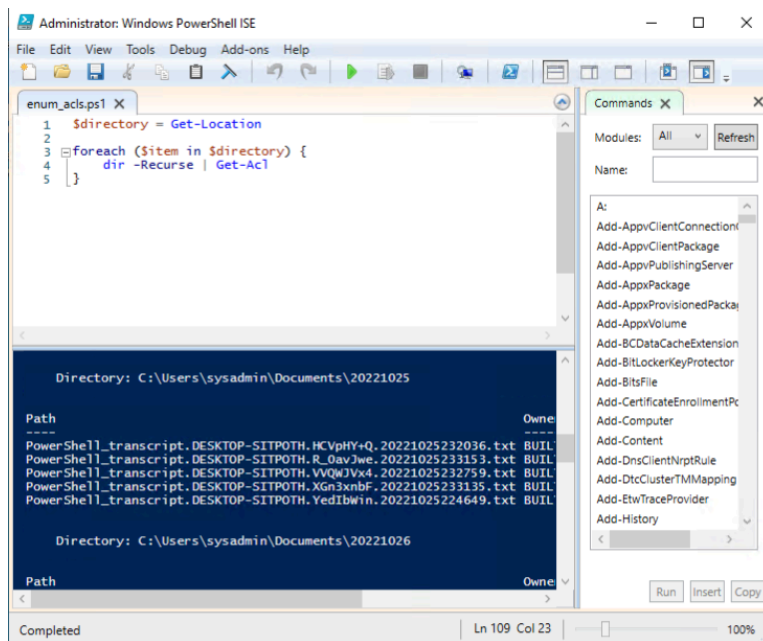


Figure 5.

Sample output of running script in cd C:\Windows:

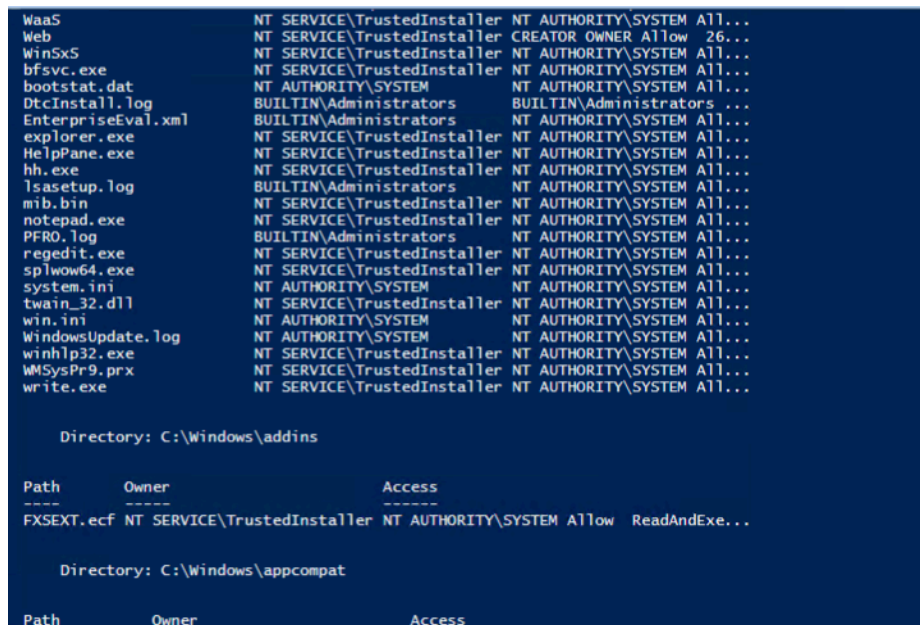
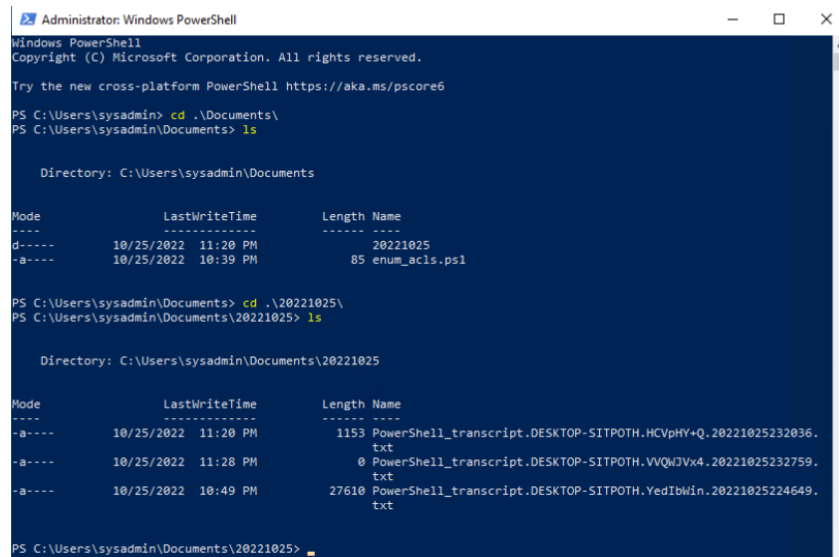


Figure 6.

## Deliverable for Bonus Task 5:

### PowerShell-logs:



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

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

Directory: C:\Users\sysadmin\Documents

Mode                LastWriteTime         Length Name
----                -
d-----          10/25/2022  11:20 PM             20221025
-a-----          10/25/2022  10:39 PM             85 enum_acis.ps1

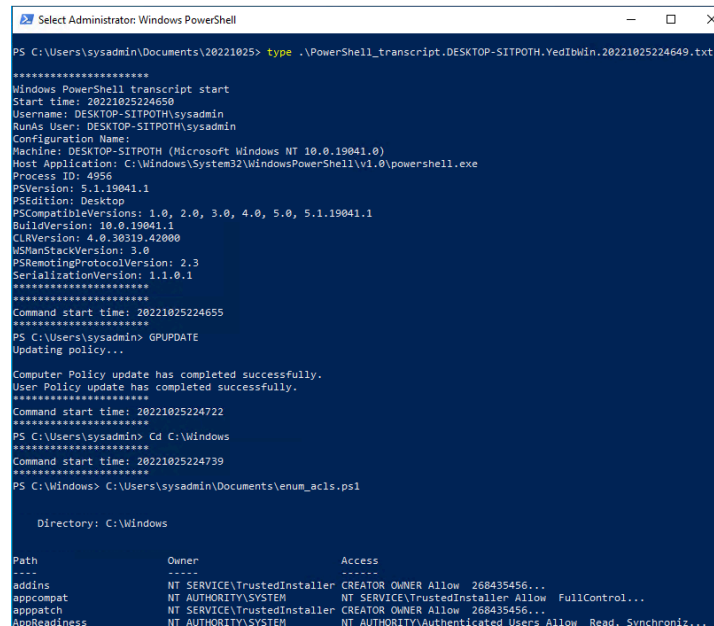
PS C:\Users\sysadmin\Documents> cd .\20221025\
PS C:\Users\sysadmin\Documents\20221025> ls

Directory: C:\Users\sysadmin\Documents\20221025

Mode                LastWriteTime         Length Name
----                -
-a-----          10/25/2022  11:20 PM          1153 PowerShell_transcript.DESKTOP-SITPOTH.HCVpHY+Q.20221025232036.
txt
-a-----          10/25/2022  11:28 PM             0 PowerShell_transcript.DESKTOP-SITPOTH.VVQWJVx4.20221025232759.
txt
-a-----          10/25/2022  10:49 PM          27610 PowerShell_transcript.DESKTOP-SITPOTH.YedIbWIn.20221025224649.
txt

PS C:\Users\sysadmin\Documents\20221025>
```

Figure 7.



```
Select Administrator: Windows PowerShell
PS C:\Users\sysadmin\Documents\20221025> type .\PowerShell_transcript.DESKTOP-SITPOTH.YedIbWIn.20221025224649.txt
*****
Windows PowerShell transcript start
Start time: 20221025224650
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: 4956
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: 20221025224655
*****
PS C:\Users\sysadmin> GPUPDATE
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.
*****
Command start time: 20221025224722
*****
PS C:\Users\sysadmin> Cd C:\Windows
*****
Command start time: 20221025224739
*****
PS C:\Windows> C:\Users\sysadmin\Documents\enum_acis.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, Synchroniz...
```

Figure 8.

```

Select Administrator: Windows PowerShell

ShellExperiences NT SERVICE\TrustedInstaller CREATOR OWNER Allow 268435456...
SKB NT SERVICE\TrustedInstaller CREATOR OWNER Allow 268435456...
SoftwareDistribution NT AUTHORITY\SYSTEM NT SERVICE\TrustedInstaller Allow FullControl...
Speech NT SERVICE\TrustedInstaller CREATOR OWNER Allow 268435456...
Speech_OneCore NT SERVICE\TrustedInstaller CREATOR OWNER Allow 268435456...
System NT SERVICE\TrustedInstaller CREATOR OWNER Allow 268435456...
System32 NT SERVICE\TrustedInstaller CREATOR OWNER Allow 268435456...
SystemApps NT AUTHORITY\SYSTEM NT SERVICE\TrustedInstaller Allow FullControl...
SystemResources NT SERVICE\TrustedInstaller NT AUTHORITY\SYSTEM Allow -1610612736...
SysWOW64 NT SERVICE\TrustedInstaller CREATOR OWNER Allow 268435456...
TAPI NT AUTHORITY\SYSTEM NT AUTHORITY\SYSTEM Allow 268435456...
Tasks NT AUTHORITY\SYSTEM CREATOR OWNER Allow 268435456...
Temp NT AUTHORITY\SYSTEM CREATOR OWNER Allow 268435456...
tracing NT AUTHORITY\SYSTEM NT AUTHORITY\SYSTEM Allow FullControl...
twain_32 NT SERVICE\TrustedInstaller CREATOR OWNER Allow 268435456...
Vss NT AUTHORITY\SYSTEM NT AUTHORITY\LOCAL SERVICE Allow FullControl...
Waa5 NT SERVICE\TrustedInstaller NT AUTHORITY\SYSTEM Allow -1610612736...
Web NT SERVICE\TrustedInstaller CREATOR OWNER Allow 268435456...
WinSxS NT SERVICE\TrustedInstaller NT AUTHORITY\SYSTEM Allow -1610612736...
bfsvc.exe NT SERVICE\TrustedInstaller NT AUTHORITY\SYSTEM Allow ReadAndExecute, Synchronize...
bootstat.dat NT AUTHORITY\SYSTEM NT AUTHORITY\SYSTEM Allow FullControl...
DtcInstall.log BUILTIN\Administrators BUILTIN\Administrators Allow FullControl...
EnterpriseEval.xml BUILTIN\Administrators NT AUTHORITY\SYSTEM Allow FullControl...
explorer.exe NT SERVICE\TrustedInstaller NT AUTHORITY\SYSTEM Allow ReadAndExecute, Synchronize...
HelpPane.exe NT SERVICE\TrustedInstaller NT AUTHORITY\SYSTEM Allow ReadAndExecute, Synchronize...
hh.exe NT SERVICE\TrustedInstaller NT AUTHORITY\SYSTEM Allow ReadAndExecute, Synchronize...
issasetup.log BUILTIN\Administrators NT AUTHORITY\SYSTEM Allow FullControl...
mb.bin NT SERVICE\TrustedInstaller NT AUTHORITY\SYSTEM Allow ReadAndExecute, Synchronize...
notepad.exe NT SERVICE\TrustedInstaller NT AUTHORITY\SYSTEM Allow ReadAndExecute, Synchronize...
PFRO.log BUILTIN\Administrators NT AUTHORITY\SYSTEM Allow FullControl...
regedit.exe NT SERVICE\TrustedInstaller NT AUTHORITY\SYSTEM Allow ReadAndExecute, Synchronize...
splwow64.exe NT SERVICE\TrustedInstaller NT AUTHORITY\SYSTEM Allow ReadAndExecute, Synchronize...
system.ini NT AUTHORITY\SYSTEM NT AUTHORITY\SYSTEM Allow FullControl...
twain_32.dll NT SERVICE\TrustedInstaller NT AUTHORITY\SYSTEM Allow ReadAndExecute, Synchronize...
win.ini NT AUTHORITY\SYSTEM NT AUTHORITY\SYSTEM Allow FullControl...
WindowsUpdate.log NT AUTHORITY\SYSTEM NT AUTHORITY\SYSTEM Allow FullControl...
winhlp32.exe NT SERVICE\TrustedInstaller NT AUTHORITY\SYSTEM Allow ReadAndExecute, Synchronize...
WMSysPr9.prx NT SERVICE\TrustedInstaller NT AUTHORITY\SYSTEM Allow ReadAndExecute, Synchronize...
write.exe NT SERVICE\TrustedInstaller NT AUTHORITY\SYSTEM Allow ReadAndExecute, Synchronize...

*****
Command start time: 20221025224753
*****
PS C:\Windows> cd C:\Users\sysadmin\Documents
*****
Command start time: 20221025224755
*****

```

Figure 9.