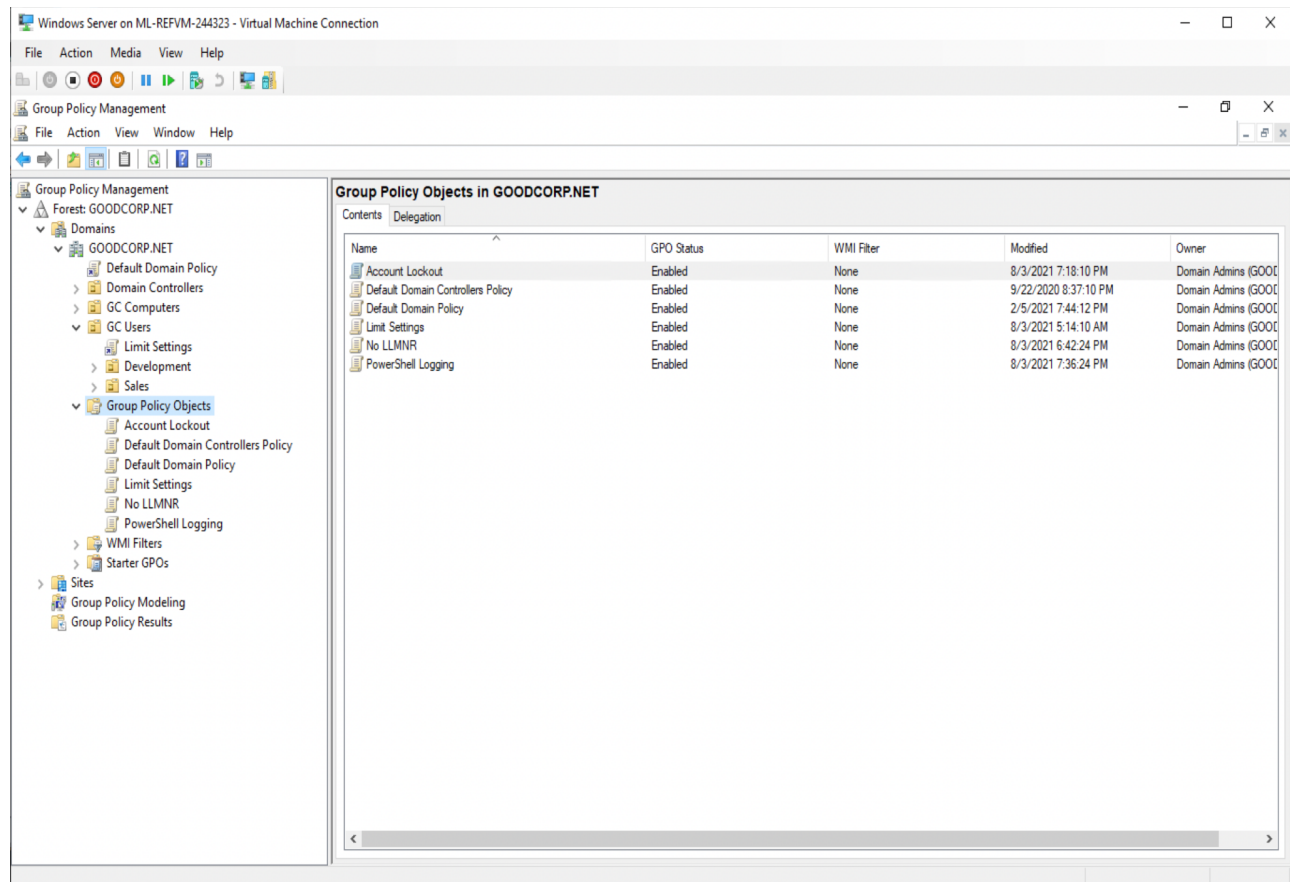
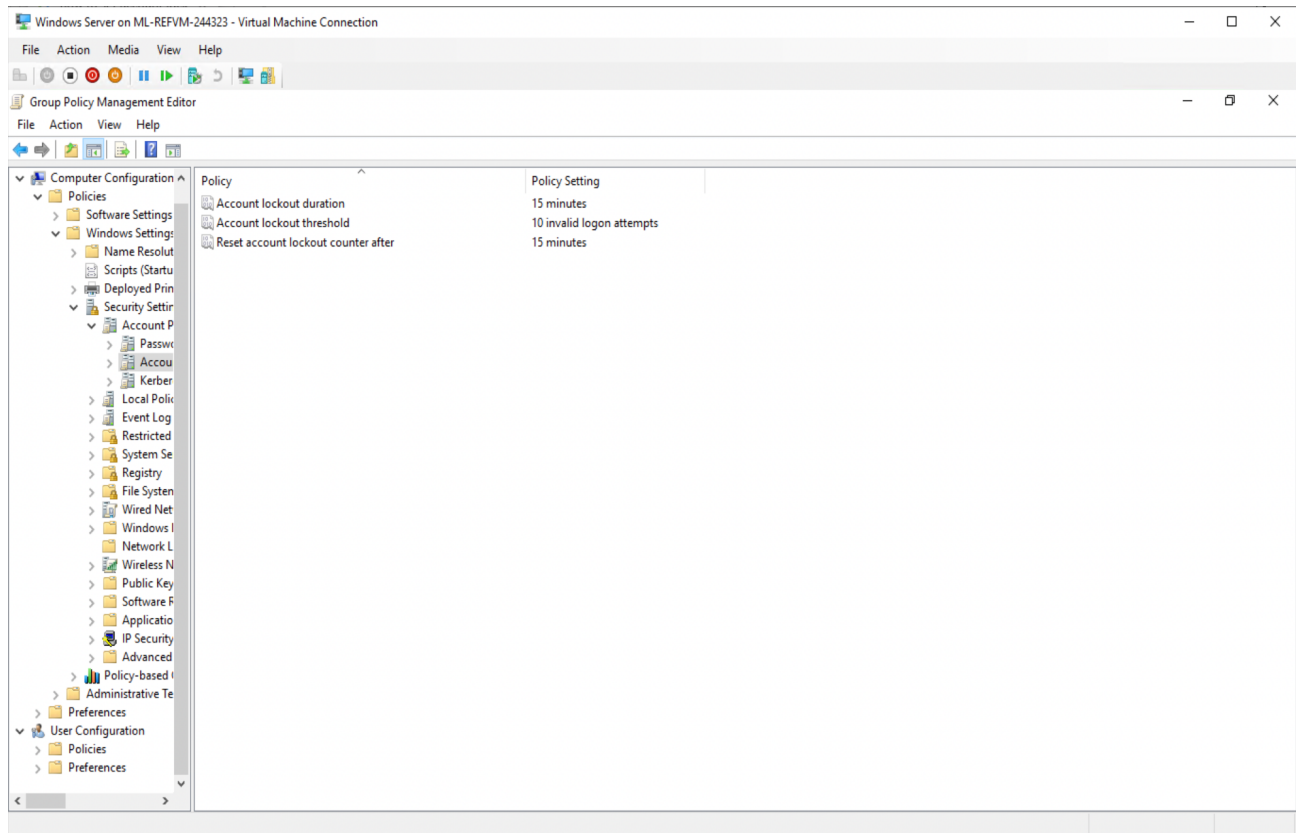


Week 7 Homework: A Day in the Life of a Windows Sysadmin

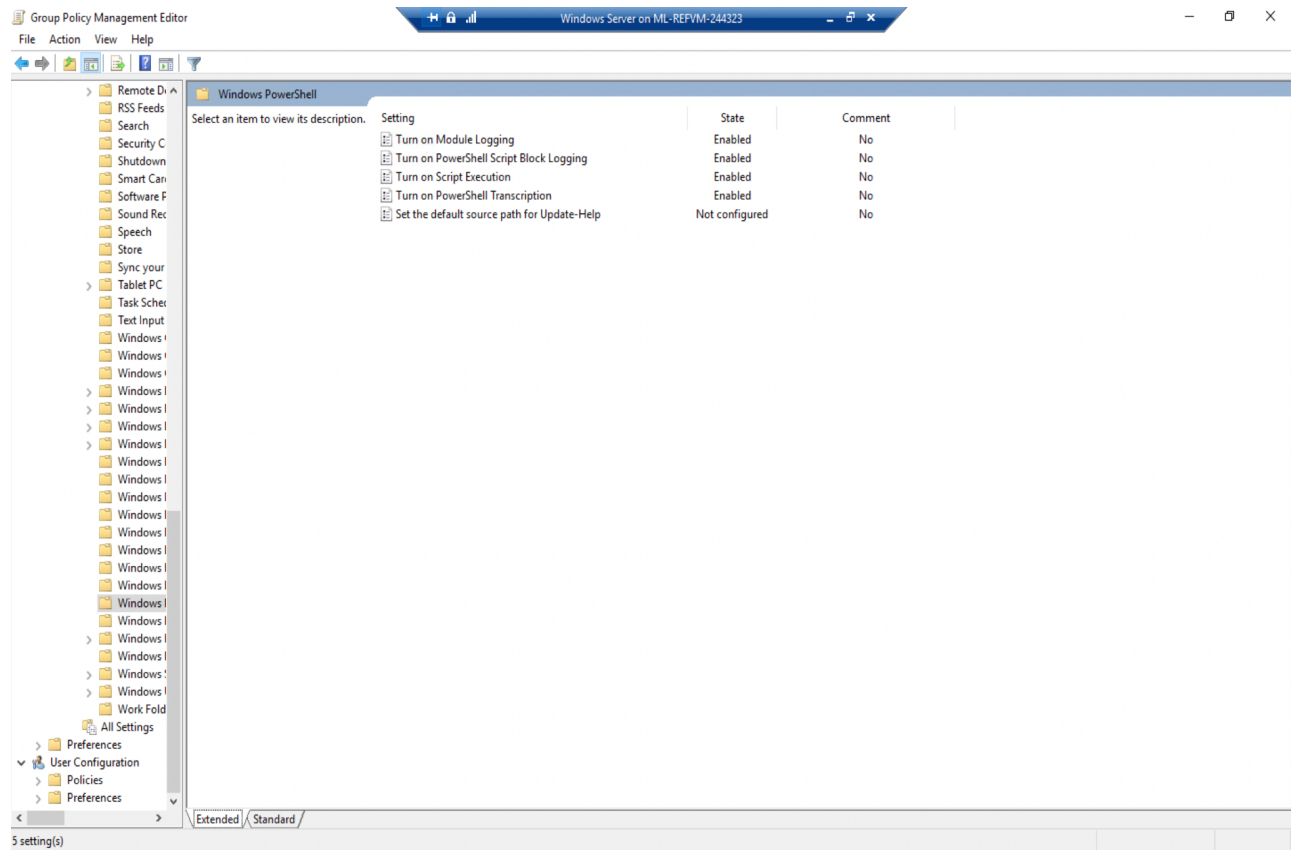
Deliverable for Task 1: Take a screenshot of all the GPOs created for this homework assignment. To find these, launch the Group Policy Management tool, select **Group Policy Objects**, and take a screenshot of the GPOs you've created.



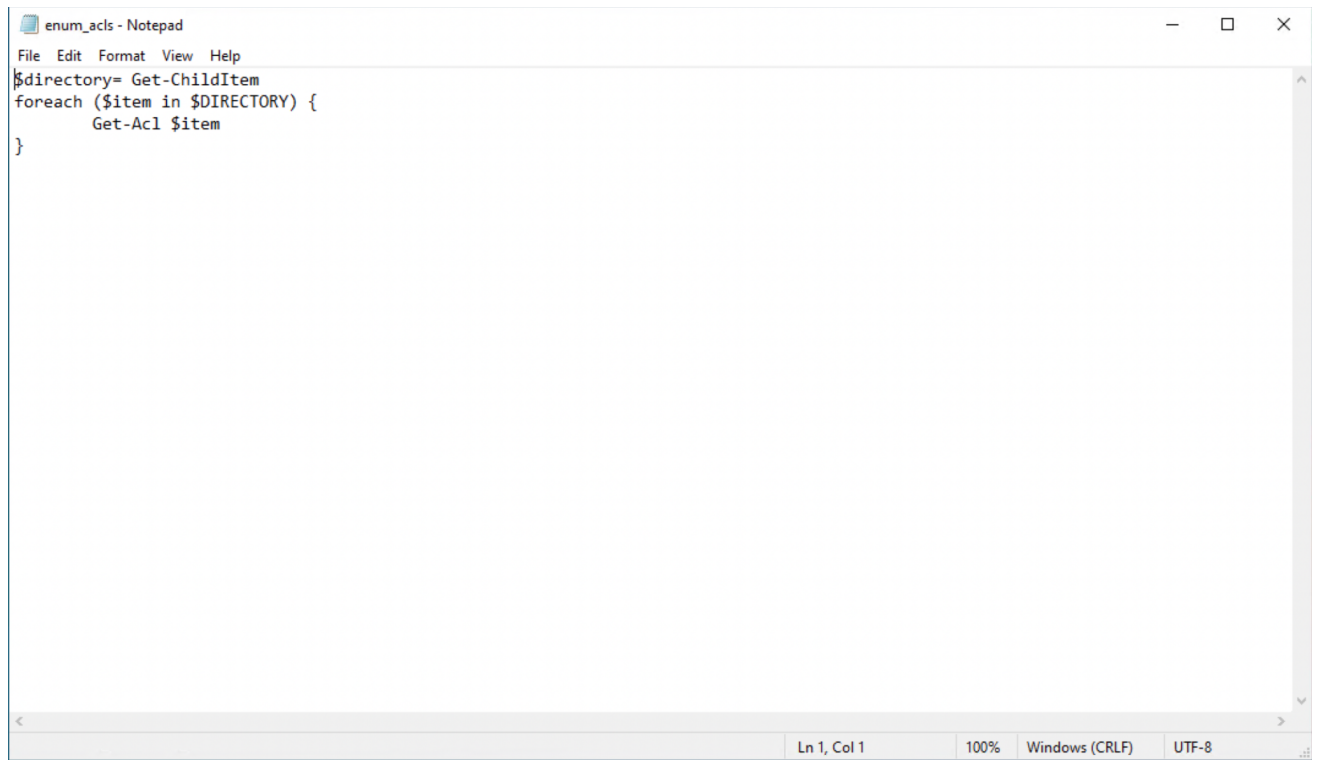
Deliverable for Task 2: Submit a screenshot of the different Account Lockout policies in Group Policy Management Editor. It should show the three values you set under the Policy and Policy Setting columns.



Deliverable for Task 3: Submit a screenshot of the different Windows PowerShell policies within the Group Policy Management Editor. Four of these should be enabled.



Deliverable for Task 4: Submit a copy of your enum_acls.ps1 script.



```
enum_acls - Notepad
File Edit Format View Help
$directory= Get-ChildItem
foreach ($item in $DIRECTORY) {
    Get-Acl $item
}
```

Ln 1, Col 1 100% Windows (CRLF) UTF-8

Deliverable for Bonus Task 5: Submit a screenshot of the contents of one of your transcribed PowerShell logs or a copy of one of the logs.

```
Select Administrator: Windows PowerShell
Windows 10 on ML-REFVM-244323

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...
DccInstall.log BUILTIN\Administrators BUILTIN\Administrators Allow FullControl...
EnterpriseEval.xml 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...
lsasetaup.log BUILTIN\Administrators NT AUTHORITY\SYSTEM Allow FullControl...
mib.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: 20210803201821
*****
PS C:\Windows> cd C:\Users\sysadmin\Documents
*****
Command start time: 20210803201830
*****
PS C:\Users\sysadmin\Documents> ls

Directory: C:\Users\sysadmin\Documents

Mode                LastWriteTime         Length Name
----                -
d-----          8/3/2021   8:11 PM             20210803
-a----          8/3/2021   8:02 PM              78 enum_acls.ps1

PS C:\Users\sysadmin\Documents\20210803>
```