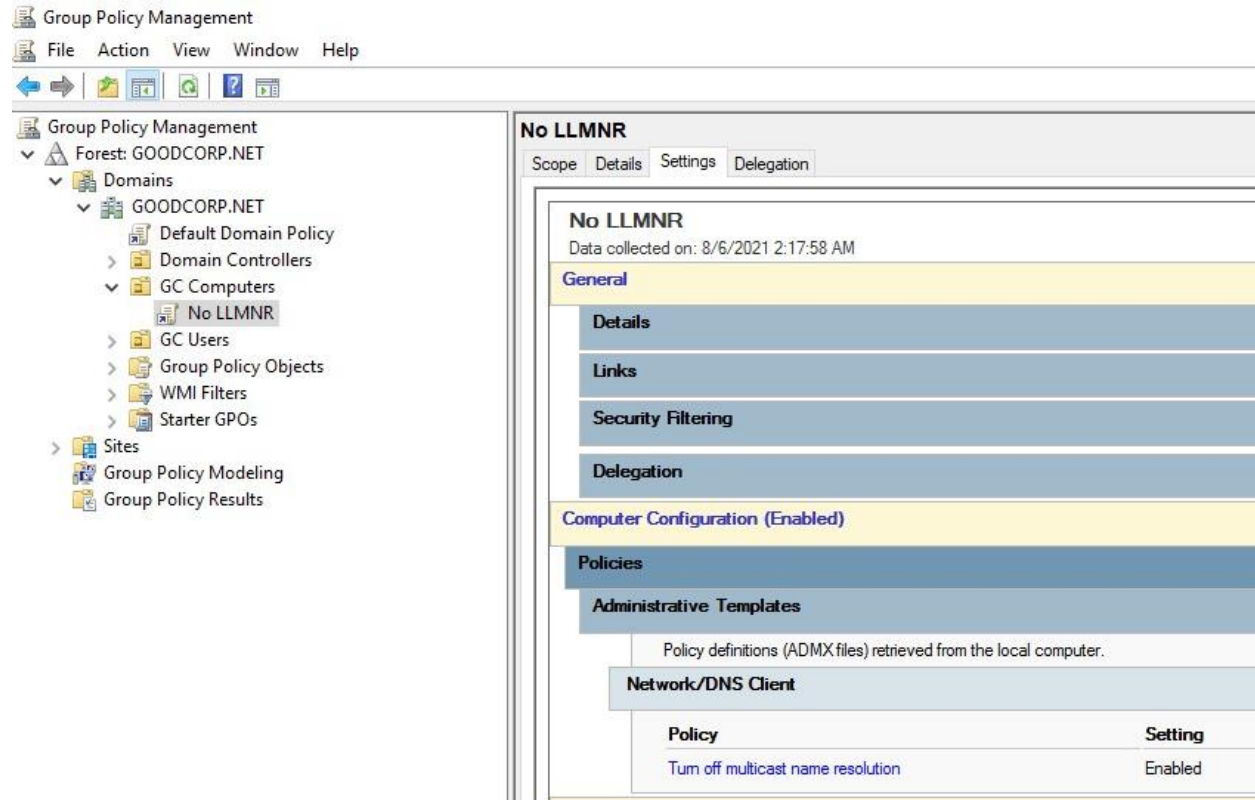
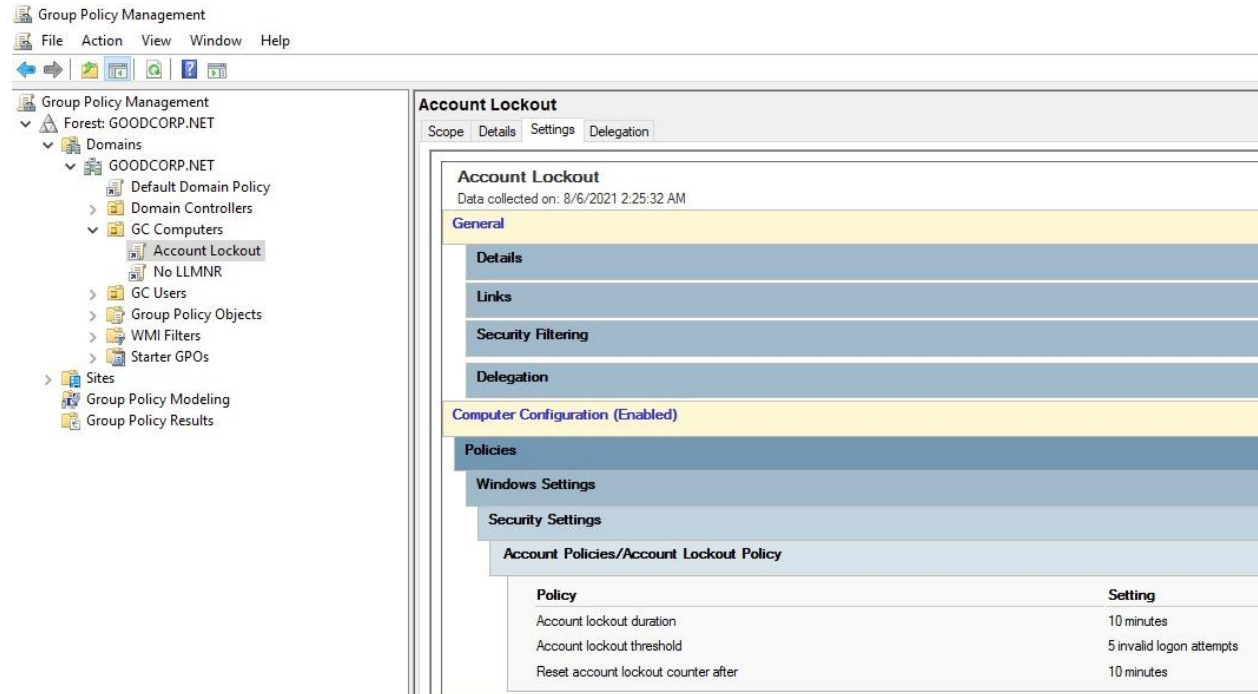


Week 7 Homework: A Day in the Life of a Windows Sysadmin

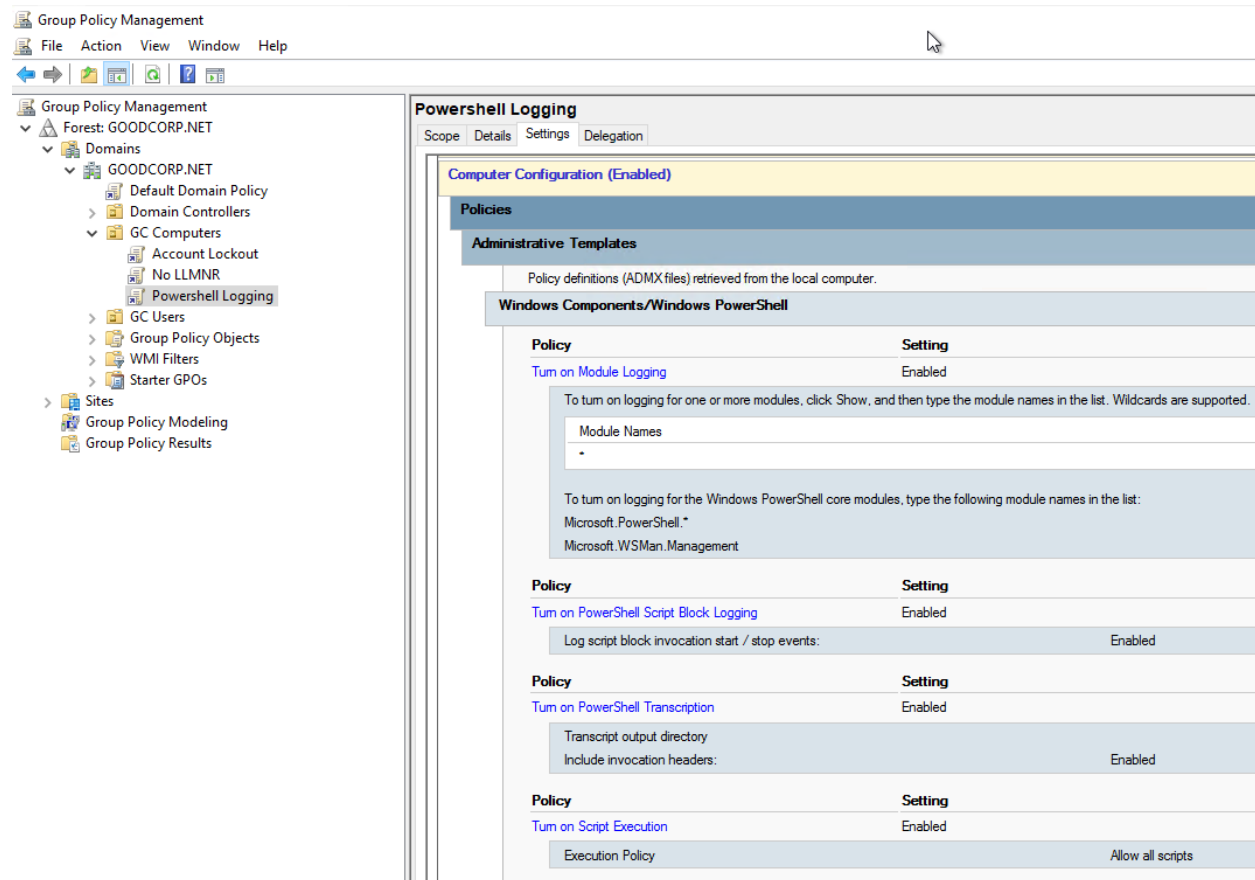
Deliverable for Task 1: Take a screenshot of all the GPOs created for this homework assignment. To find these, launch the Group Policy Management tool, select 'Group Policy Objects', and take a screenshot of the GPOs you've created.



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.



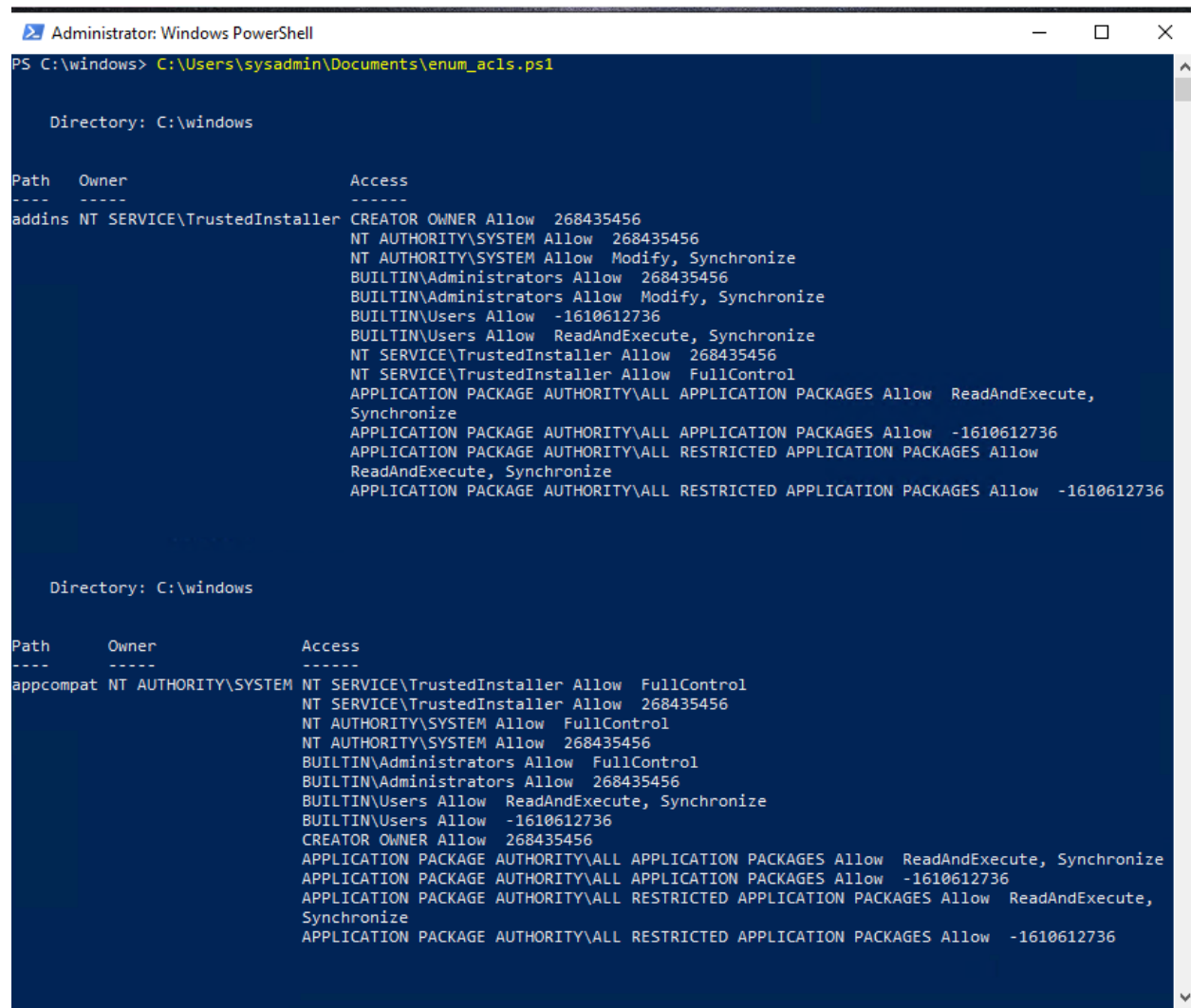
Deliverable for Task 4: Submit a copy of your `enum_acls.ps1` script.

```
foreach ($item in Get-ChildItem)
```

```
{  
    Get-Acl $item | Format-Table -Wrap  
}
```

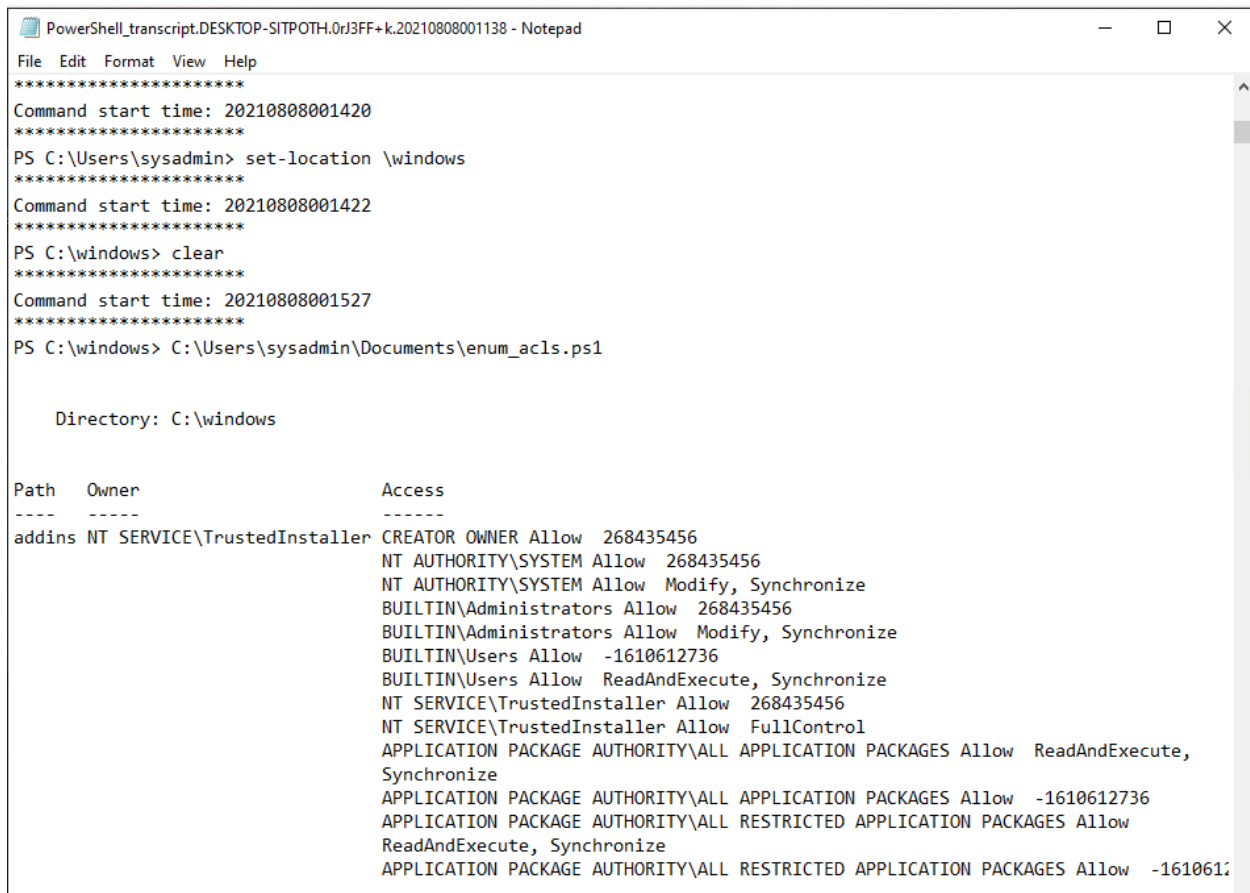
```

```



```
Administrator: Windows PowerShell  
PS C:\windows> C:\Users\sysadmin\Documents\enum_acls.ps1  
  
Directory: C:\windows  
  
Path      Owner      Access  
----      -  
addins NT SERVICE\TrustedInstaller CREATOR OWNER Allow 268435456  
NT AUTHORITY\SYSTEM Allow 268435456  
NT AUTHORITY\SYSTEM Allow Modify, Synchronize  
BUILTIN\Administrators Allow 268435456  
BUILTIN\Administrators Allow Modify, Synchronize  
BUILTIN\Users Allow -1610612736  
BUILTIN\Users Allow ReadAndExecute, Synchronize  
NT SERVICE\TrustedInstaller Allow 268435456  
NT SERVICE\TrustedInstaller Allow FullControl  
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute,  
Synchronize  
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow -1610612736  
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  
ReadAndExecute, Synchronize  
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow -1610612736  
  
Directory: C:\windows  
  
Path      Owner      Access  
----      -  
appcompat NT AUTHORITY\SYSTEM NT SERVICE\TrustedInstaller Allow FullControl  
NT SERVICE\TrustedInstaller Allow 268435456  
NT AUTHORITY\SYSTEM Allow FullControl  
NT AUTHORITY\SYSTEM Allow 268435456  
BUILTIN\Administrators Allow FullControl  
BUILTIN\Administrators Allow 268435456  
BUILTIN\Users Allow ReadAndExecute, Synchronize  
BUILTIN\Users Allow -1610612736  
CREATOR OWNER Allow 268435456  
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize  
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow -1610612736  
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute,  
Synchronize  
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow -1610612736
```

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.



```
PowerShell_transcript.DESKTOP-SITPOTH.0rj3FF+k.20210808001138 - Notepad
File Edit Format View Help
*****
Command start time: 20210808001420
*****
PS C:\Users\sysadmin> set-location \windows
*****
Command start time: 20210808001422
*****
PS C:\windows> clear
*****
Command start time: 20210808001527
*****
PS C:\windows> C:\Users\sysadmin\Documents\enum_acls.ps1

Directory: C:\windows

Path      Owner
----
addins NT SERVICE\TrustedInstaller
Access
-----
CREATOR OWNER Allow 268435456
NT AUTHORITY\SYSTEM Allow 268435456
NT AUTHORITY\SYSTEM Allow Modify, Synchronize
BUILTIN\Administrators Allow 268435456
BUILTIN\Administrators Allow Modify, Synchronize
BUILTIN\Users Allow -1610612736
BUILTIN\Users Allow ReadAndExecute, Synchronize
NT SERVICE\TrustedInstaller Allow 268435456
NT SERVICE\TrustedInstaller Allow FullControl
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute,
Synchronize
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow -1610612736
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow
ReadAndExecute, Synchronize
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow -1610612
```