

Student:

Jacob Jeffers

Email:

jjeffers6151@ucumberlands.edu

Time on Task:

18 hours, 55 minutes

Progress:

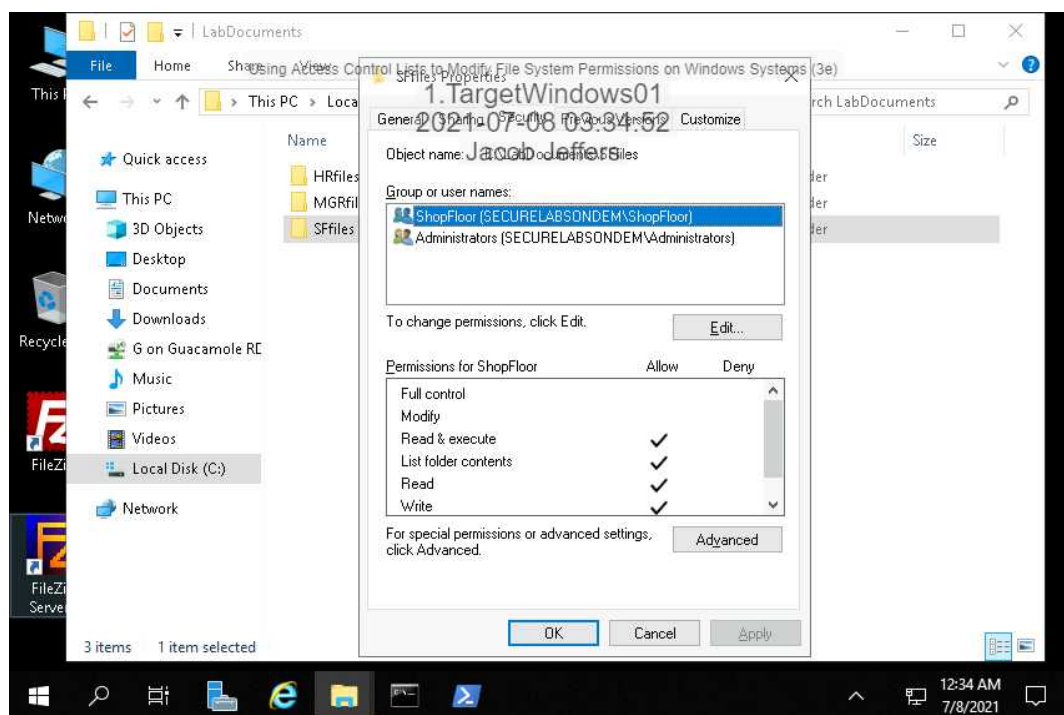
100%

Report Generated: Thursday, July 8, 2021 at 4:59 AM

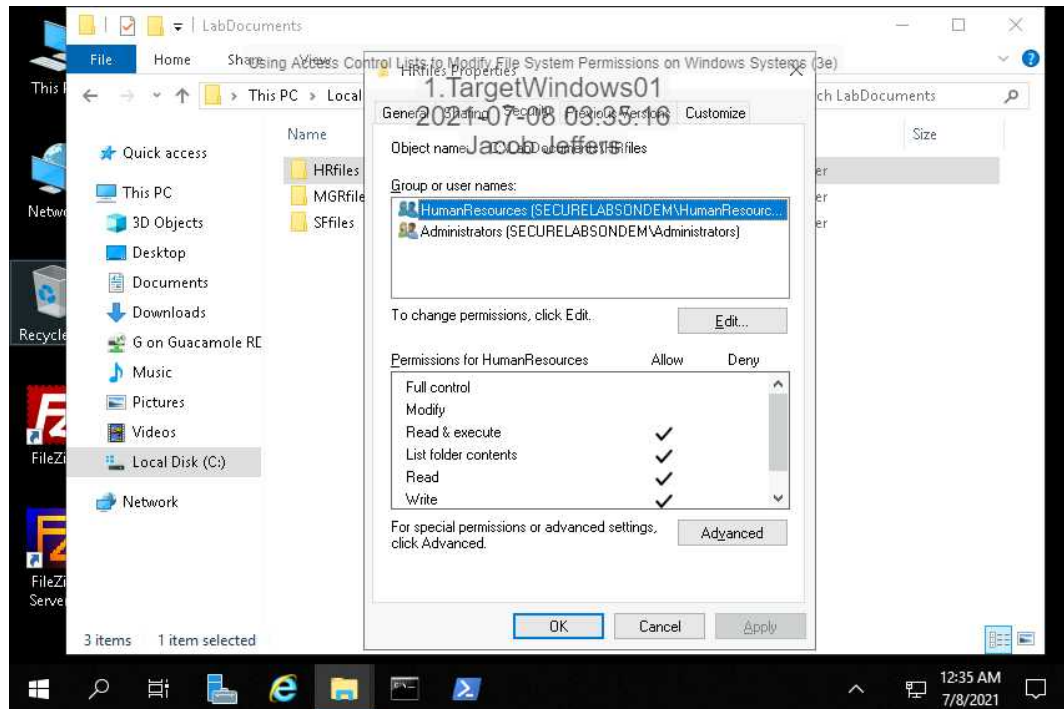
Section 1: Hands-On Demonstration

Part 1: View Existing ACLs on a Windows System

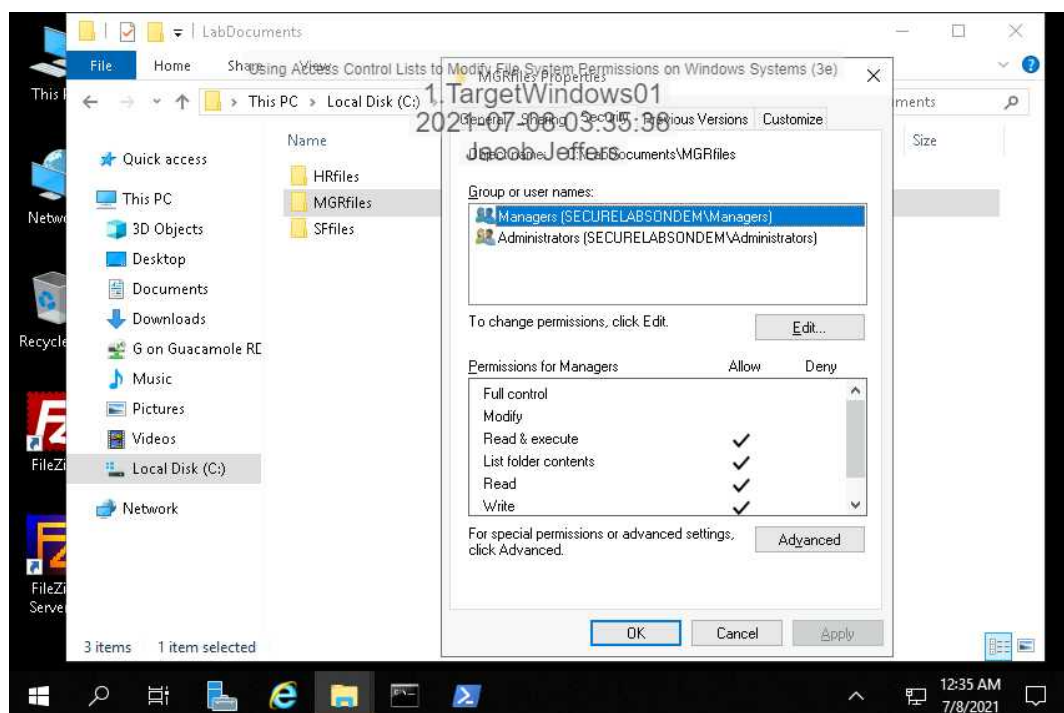
5. Make a screen capture showing the **current permissions for the SFfiles folder**.



12. Make a screen capture showing the current permissions for the HRfiles folder.



15. Make a screen capture showing the current permissions for the MGRfiles folder.



Part 2: Modify ACLs using Icacs.exe

8. **Compare the results** of the `icacls.exe` command with the ACLs you reviewed in Part 1 of this lab. Do they match?

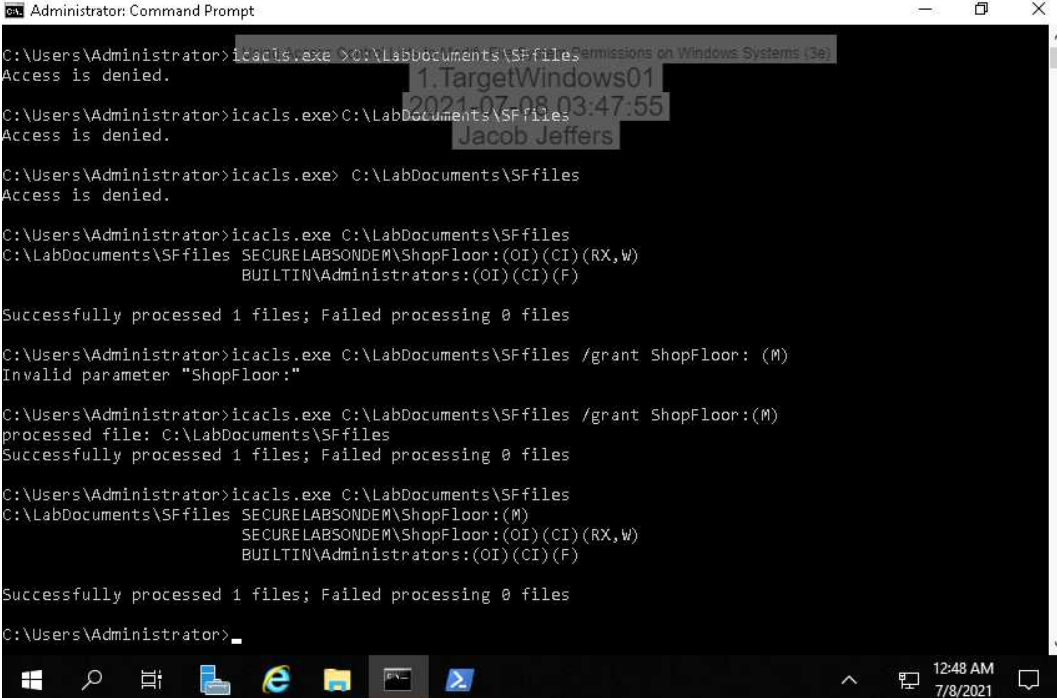
They do match. ShopFloor is able to read, write, and execute in both parts.

11. **Compare the new results** of this command with the results from step 7.

You should notice that there is now a new line item for SECURELABSONDEM\ShopFloor. The `grant` command creates a new line item for any principal with permissions added through `icacls.exe`; technically, `icacls.exe` adds “special” permissions, which are visible by clicking the Advanced button in the folder Properties dialog box.

There is a new line which shows that ShopFloor has access to modify within the SFfiles folder.

12. **Make a screen capture** showing the **changes you made to the SFfiles folder permissions**.



```
Administrator: Command Prompt
C:\Users\Administrator>icacls.exe >C:\LabDocuments\SFfiles
Access is denied.

C:\Users\Administrator>icacls.exe C:\LabDocuments\SFfiles
Access is denied.

C:\Users\Administrator>icacls.exe C:\LabDocuments\SFfiles
Access is denied.

C:\Users\Administrator>icacls.exe C:\LabDocuments\SFfiles
C:\LabDocuments\SFfiles  SECURELABSONDEM\ShopFloor:(OI)(CI)(RX,W)
                        BUILTIN\Administrators:(OI)(CI)(F)

Successfully processed 1 files; Failed processing 0 files

C:\Users\Administrator>icacls.exe C:\LabDocuments\SFfiles /grant ShopFloor:(M)
Invalid parameter "ShopFloor:"

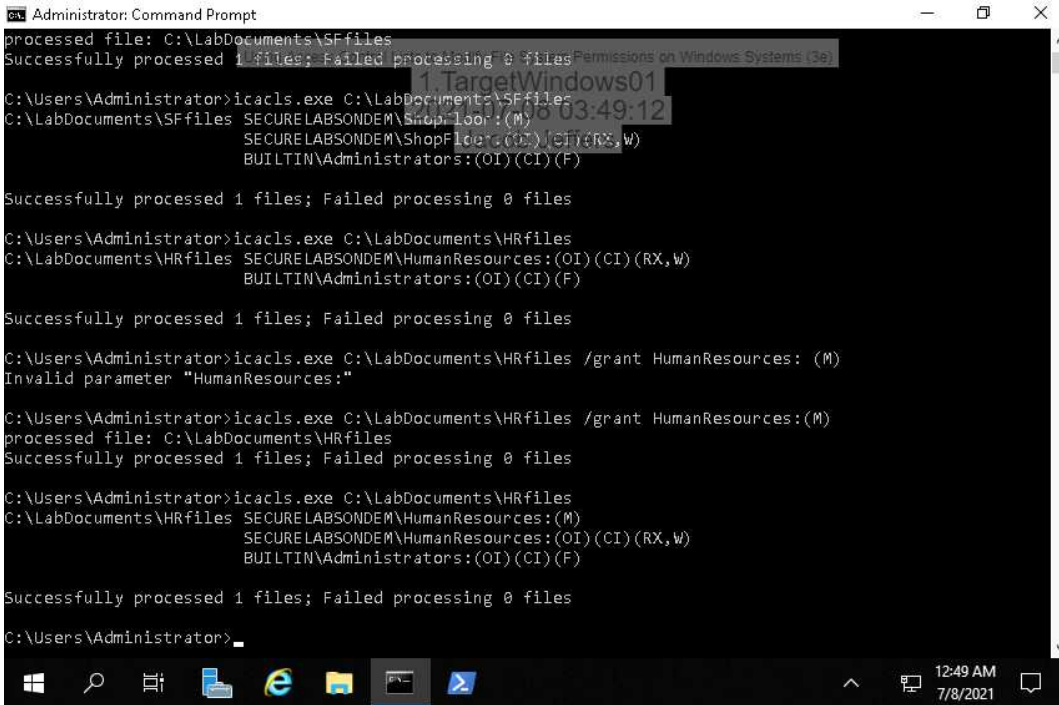
C:\Users\Administrator>icacls.exe C:\LabDocuments\SFfiles /grant ShopFloor:(M)
processed file: C:\LabDocuments\SFfiles
Successfully processed 1 files; Failed processing 0 files

C:\Users\Administrator>icacls.exe C:\LabDocuments\SFfiles
C:\LabDocuments\SFfiles  SECURELABSONDEM\ShopFloor:(M)
                        SECURELABSONDEM\ShopFloor:(OI)(CI)(RX,W)
                        BUILTIN\Administrators:(OI)(CI)(F)

Successfully processed 1 files; Failed processing 0 files

C:\Users\Administrator>
```

14. Make a screen capture showing the changes you made to the HRfiles folder permissions.



```
Administrator: Command Prompt
processed file: C:\LabDocuments\SFfiles
Successfully processed 1 files; Failed processing 0 files

C:\Users\Administrator>icacls.exe C:\LabDocuments\SFfiles
C:\LabDocuments\SFfiles  SECURELABSONDEM\Shop:100:(M)
                        SECURELABSONDEM\Shop:File:(CI)(CI)(RX,W)
                        BUILTIN\Administrators:(OI)(CI)(F)

Successfully processed 1 files; Failed processing 0 files

C:\Users\Administrator>icacls.exe C:\LabDocuments\HRfiles
C:\LabDocuments\HRfiles  SECURELABSONDEM\HumanResources:(OI)(CI)(RX,W)
                        BUILTIN\Administrators:(OI)(CI)(F)

Successfully processed 1 files; Failed processing 0 files

C:\Users\Administrator>icacls.exe C:\LabDocuments\HRfiles /grant HumanResources:(M)
Invalid parameter "HumanResources:"

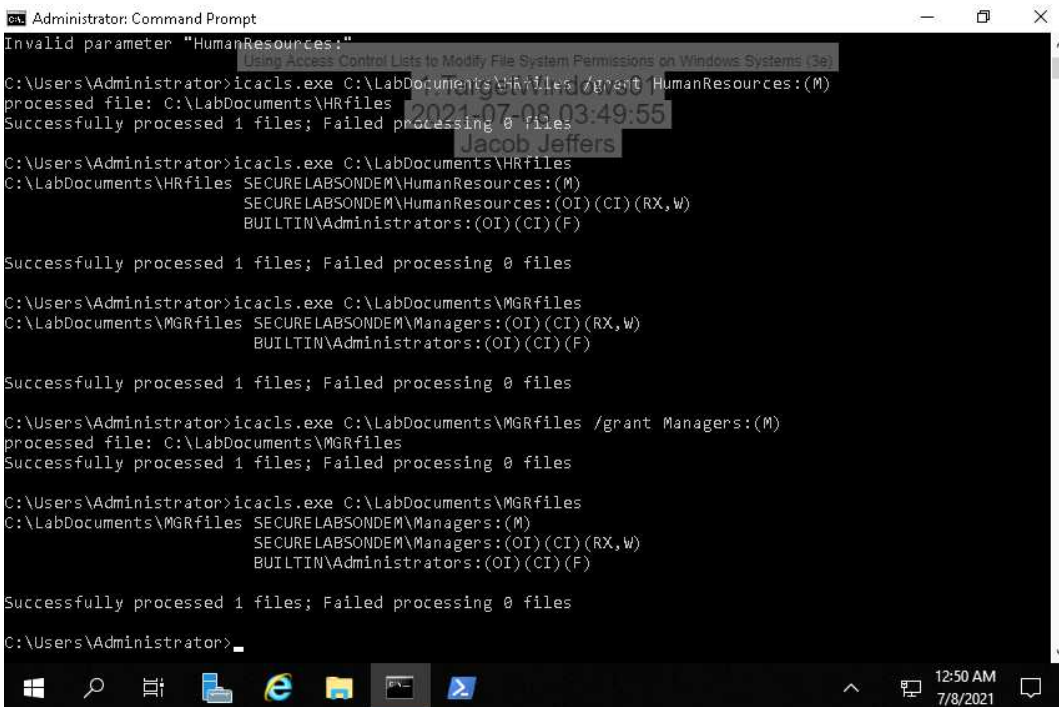
C:\Users\Administrator>icacls.exe C:\LabDocuments\HRfiles /grant HumanResources:(M)
processed file: C:\LabDocuments\HRfiles
Successfully processed 1 files; Failed processing 0 files

C:\Users\Administrator>icacls.exe C:\LabDocuments\HRfiles
C:\LabDocuments\HRfiles  SECURELABSONDEM\HumanResources:(M)
                        SECURELABSONDEM\HumanResources:(OI)(CI)(RX,W)
                        BUILTIN\Administrators:(OI)(CI)(F)

Successfully processed 1 files; Failed processing 0 files

C:\Users\Administrator>
```

16. Make a screen capture showing the changes you made to the MGRfiles folder permissions.



```
Administrator: Command Prompt
Invalid parameter "HumanResources:"

C:\Users\Administrator>icacls.exe C:\LabDocuments\HRfiles /grant HumanResources:(M)
processed file: C:\LabDocuments\HRfiles
Successfully processed 1 files; Failed processing 0 files

C:\Users\Administrator>icacls.exe C:\LabDocuments\HRfiles
C:\LabDocuments\HRfiles  SECURELABSONDEM\HumanResources:(M)
                        SECURELABSONDEM\HumanResources:(OI)(CI)(RX,W)
                        BUILTIN\Administrators:(OI)(CI)(F)

Successfully processed 1 files; Failed processing 0 files

C:\Users\Administrator>icacls.exe C:\LabDocuments\MGRfiles
C:\LabDocuments\MGRfiles  SECURELABSONDEM\Managers:(OI)(CI)(RX,W)
                        BUILTIN\Administrators:(OI)(CI)(F)

Successfully processed 1 files; Failed processing 0 files

C:\Users\Administrator>icacls.exe C:\LabDocuments\MGRfiles /grant Managers:(M)
processed file: C:\LabDocuments\MGRfiles
Successfully processed 1 files; Failed processing 0 files

C:\Users\Administrator>icacls.exe C:\LabDocuments\MGRfiles
C:\LabDocuments\MGRfiles  SECURELABSONDEM\Managers:(M)
                        SECURELABSONDEM\Managers:(OI)(CI)(RX,W)
                        BUILTIN\Administrators:(OI)(CI)(F)

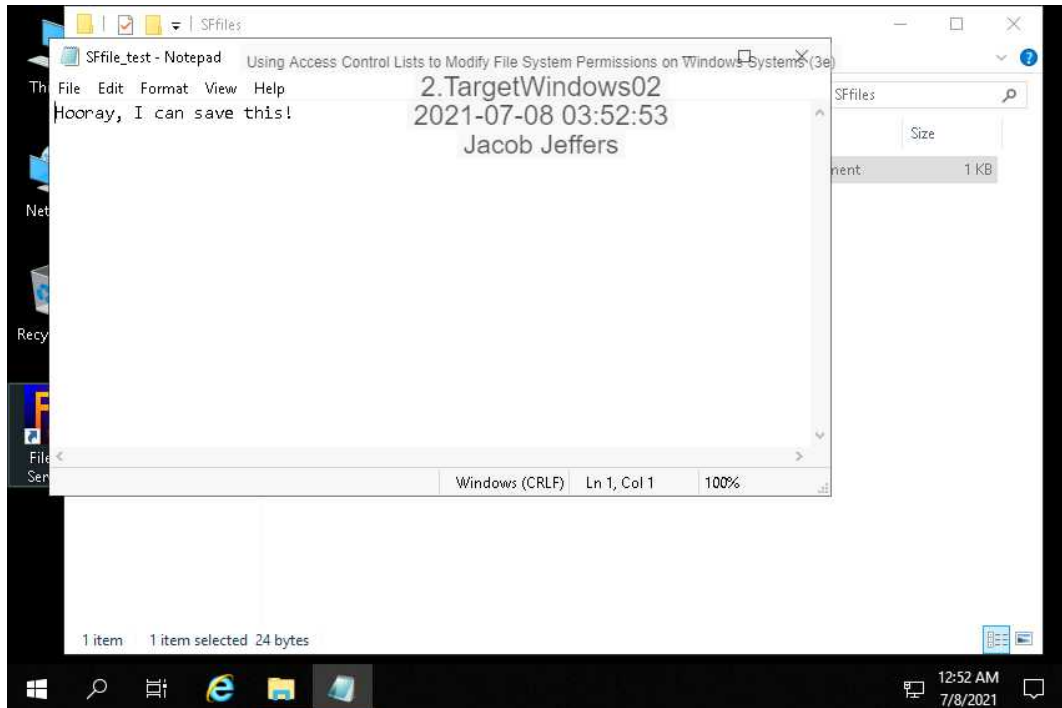
Successfully processed 1 files; Failed processing 0 files

C:\Users\Administrator>
```

Part 3: Validate ACL Settings

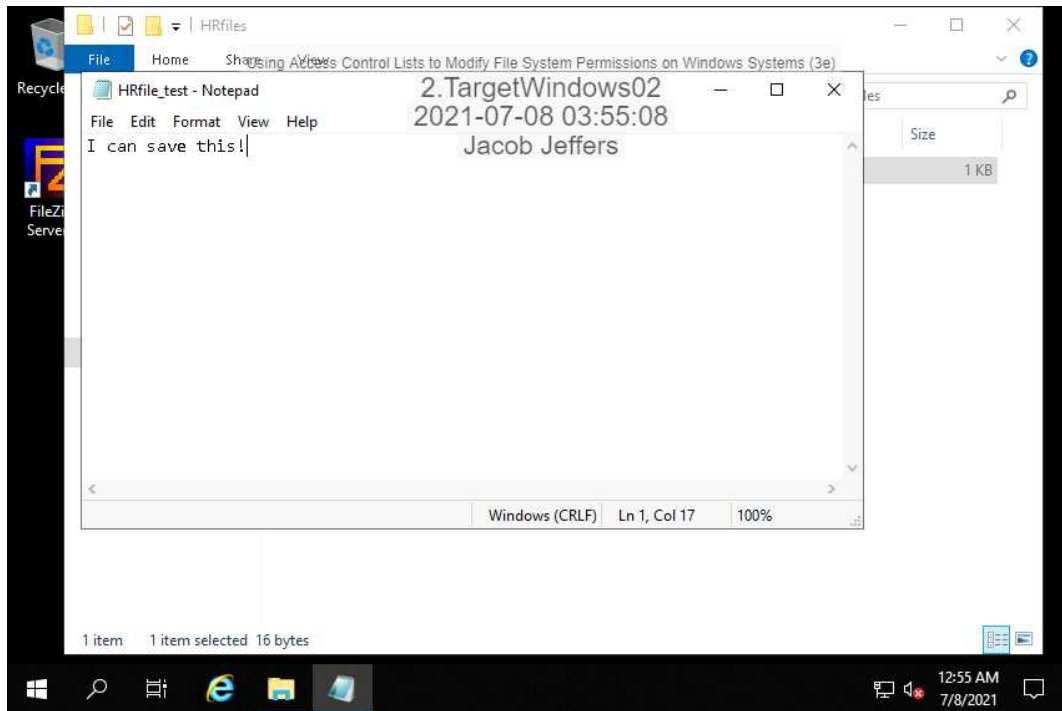
14. **Make a screen capture** showing the **modified text file** in the **SFfiles** folder.

The modified file will show a 1 KB value in the Size column, indicating that text has been added to the file.



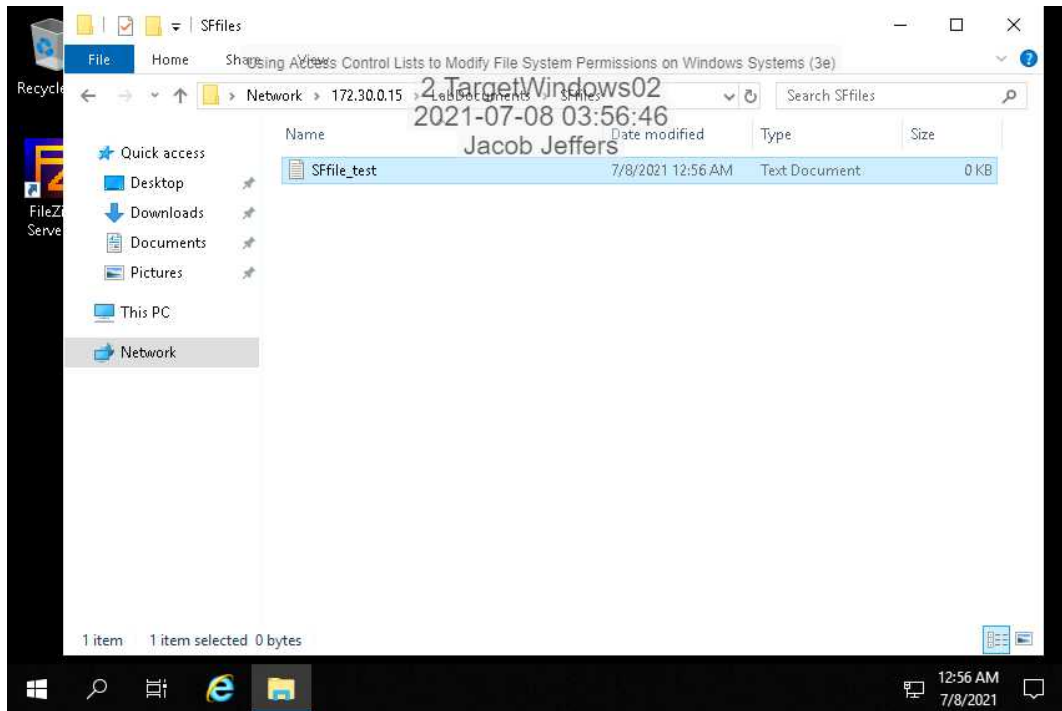
17. **Make a screen capture** showing the **modified text file in the HRfiles folder**.

The modified file will show a 1 KB value in the Size column, indicating that text has been added to the file.



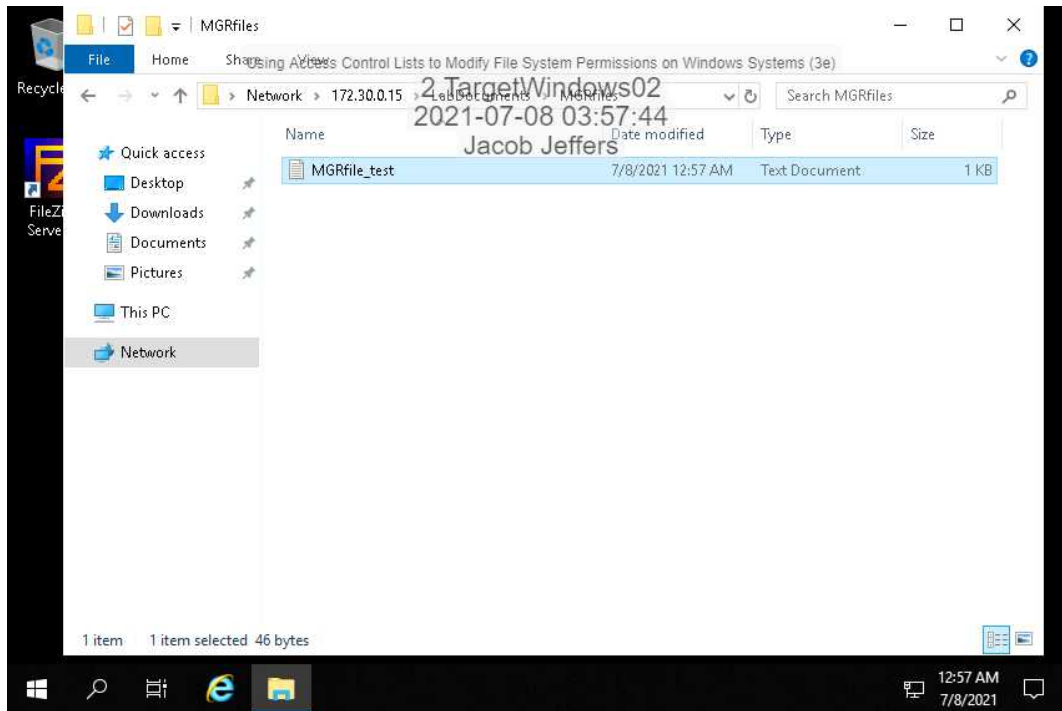
20. **Make a screen capture** showing the **re-modified text file in the SFfiles folder**.

The modified file will show a 0 KB value in the Size column, indicating that all text has been removed from the file.



21. Make a screen capture showing the **modified text file in the MGRfiles folder**.

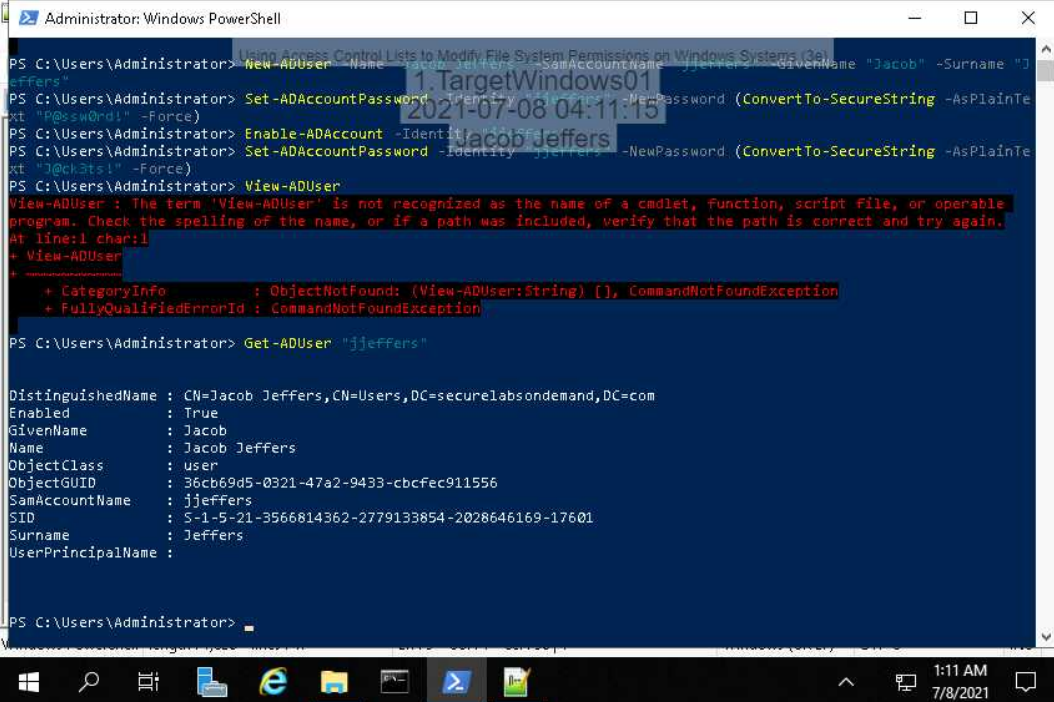
The modified file will show a 1 KB value in the Size column, indicating that text has been added to the file.



Section 2: Applied Learning

Part 1: Add a New User using a Script

3. Make a screen capture showing the new user account in this script.



The screenshot shows a Windows PowerShell window titled "Administrator: Windows PowerShell". The command prompt is at "PS C:\Users\Administrator>". The user has executed a series of commands to create a new user account. The first command is `New-ADUser -Name 'Jacob Jeffers' -SamAccountName 'jjeffers' -GivenName 'Jacob' -Surname 'Jeffers' -Password (ConvertTo-SecureString 'P@ssw0rd!' -Force)`. The second command is `Set-ADAccountPassword -Identity 'jjeffers' -NewPassword (ConvertTo-SecureString 'P@ssw0rd!' -Force)`. The third command is `Enable-ADAccount -Identity 'jjeffers'`. The fourth command is `Set-ADAccountPassword -Identity 'jjeffers' -NewPassword (ConvertTo-SecureString 'P@ssw0rd!' -Force)`. The fifth command is `View-ADUser`, which results in an error: "View-ADUser : The term 'View-ADUser' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the spelling of the name, or if a path was included, verify that the path is correct and try again. at line:1 char:1 + View-ADUser + ~~~~~ + CategoryInfo : ObjectNotFound: (View-ADUser:String) [], CommandNotFoundException + FullyQualifiedErrorId : CommandNotFoundException". The sixth command is `Get-ADUser "jjeffers"`, which returns the following properties: DistinguishedName : CN=Jacob Jeffers,CN=Users,DC=securelabsondemand,DC=com; Enabled : True; GivenName : Jacob; Name : Jacob Jeffers; ObjectClass : user; ObjectGUID : 36cb69d5-0321-47a2-9433-cbcfec911556; SamAccountName : jjeffers; SID : S-1-5-21-3566814362-2779133854-2028646169-17601; Surname : Jeffers; UserPrincipalName : . The taskbar at the bottom shows the Windows Start button, search icon, and several application icons. The system clock shows 1:11 AM on 7/8/2021.

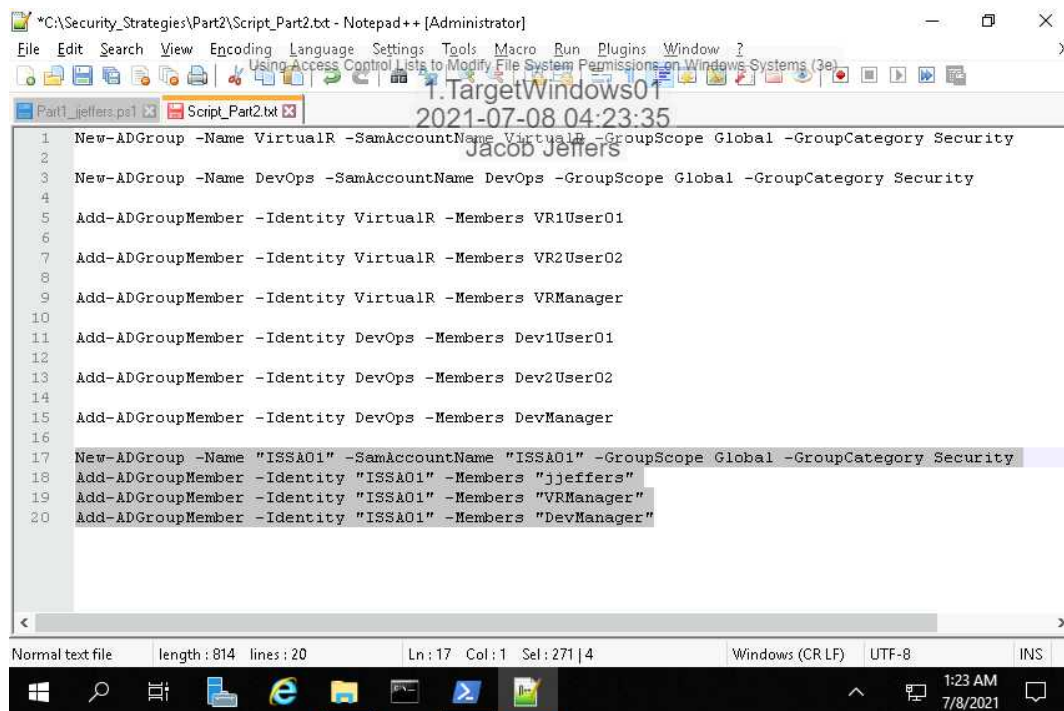
```
PS C:\Users\Administrator> New-ADUser -Name 'Jacob Jeffers' -SamAccountName 'jjeffers' -GivenName 'Jacob' -Surname 'Jeffers' -Password (ConvertTo-SecureString 'P@ssw0rd!' -Force)
PS C:\Users\Administrator> Set-ADAccountPassword -Identity 'jjeffers' -NewPassword (ConvertTo-SecureString 'P@ssw0rd!' -Force)
PS C:\Users\Administrator> Enable-ADAccount -Identity 'jjeffers'
PS C:\Users\Administrator> Set-ADAccountPassword -Identity 'jjeffers' -NewPassword (ConvertTo-SecureString 'P@ssw0rd!' -Force)
PS C:\Users\Administrator> View-ADUser
View-ADUser : The term 'View-ADUser' is not recognized as the name of a cmdlet, function, script file, or operable
program. Check the spelling of the name, or if a path was included, verify that the path is correct and try again.
at line:1 char:1
+ View-ADUser
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (View-ADUser:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException

PS C:\Users\Administrator> Get-ADUser "jjeffers"

DistinguishedName : CN=Jacob Jeffers,CN=Users,DC=securelabsondemand,DC=com
Enabled            : True
GivenName         : Jacob
Name              : Jacob Jeffers
ObjectClass       : user
ObjectGUID        : 36cb69d5-0321-47a2-9433-cbcfec911556
SamAccountName    : jjeffers
SID               : S-1-5-21-3566814362-2779133854-2028646169-17601
Surname           : Jeffers
UserPrincipalName :
```

Part 2: Add a New Group using a Script

5. Make a screen capture showing the modifications you made to the script.



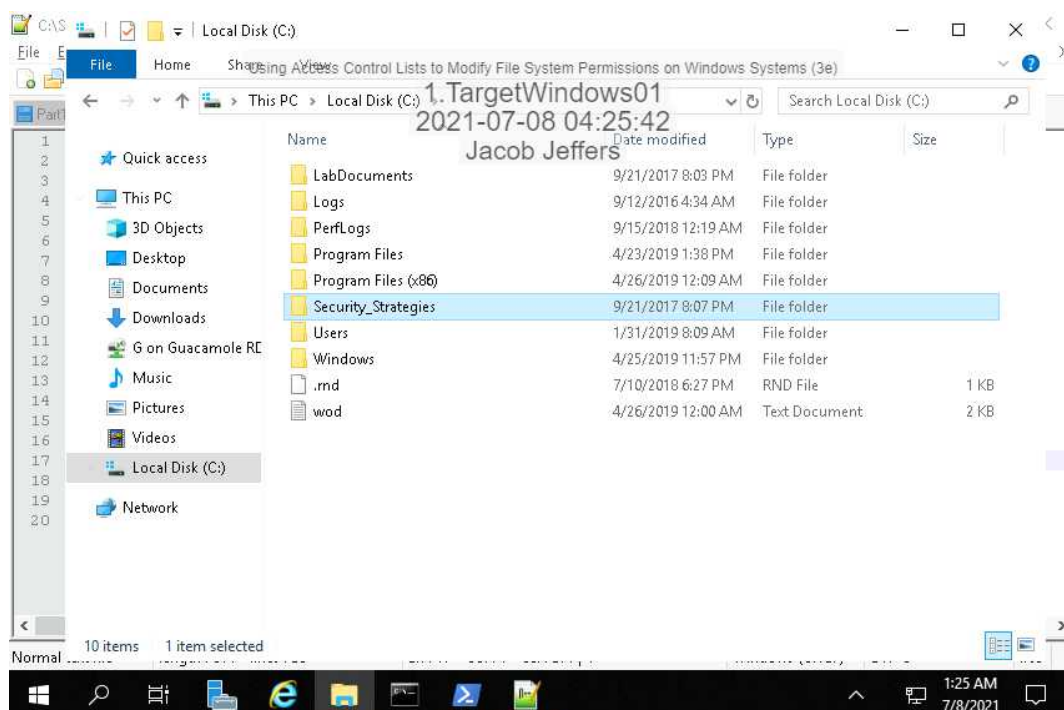
The screenshot shows a Notepad++ window titled "C:\Security_Strategies\Part2\Script_Part2.txt - Notepad++ [Administrator]". The script contains the following commands:

```
1 New-ADGroup -Name VirtualR -SamAccountName VirtualR -GroupScope Global -GroupCategory Security
2
3 New-ADGroup -Name DevOps -SamAccountName DevOps -GroupScope Global -GroupCategory Security
4
5 Add-ADGroupMember -Identity VirtualR -Members VR1User01
6
7 Add-ADGroupMember -Identity VirtualR -Members VR2User02
8
9 Add-ADGroupMember -Identity VirtualR -Members VRManager
10
11 Add-ADGroupMember -Identity DevOps -Members Dev1User01
12
13 Add-ADGroupMember -Identity DevOps -Members Dev2User02
14
15 Add-ADGroupMember -Identity DevOps -Members DevManager
16
17 New-ADGroup -Name "ISSA01" -SamAccountName "ISSA01" -GroupScope Global -GroupCategory Security
18 Add-ADGroupMember -Identity "ISSA01" -Members "jjeffers"
19 Add-ADGroupMember -Identity "ISSA01" -Members "VRManager"
20 Add-ADGroupMember -Identity "ISSA01" -Members "DevManager"
```

The status bar at the bottom indicates: Normal text file, length: 814, lines: 20, Ln: 17, Col: 1, Sel: 271 | 4, Windows (CR LF), UTF-8, INS.

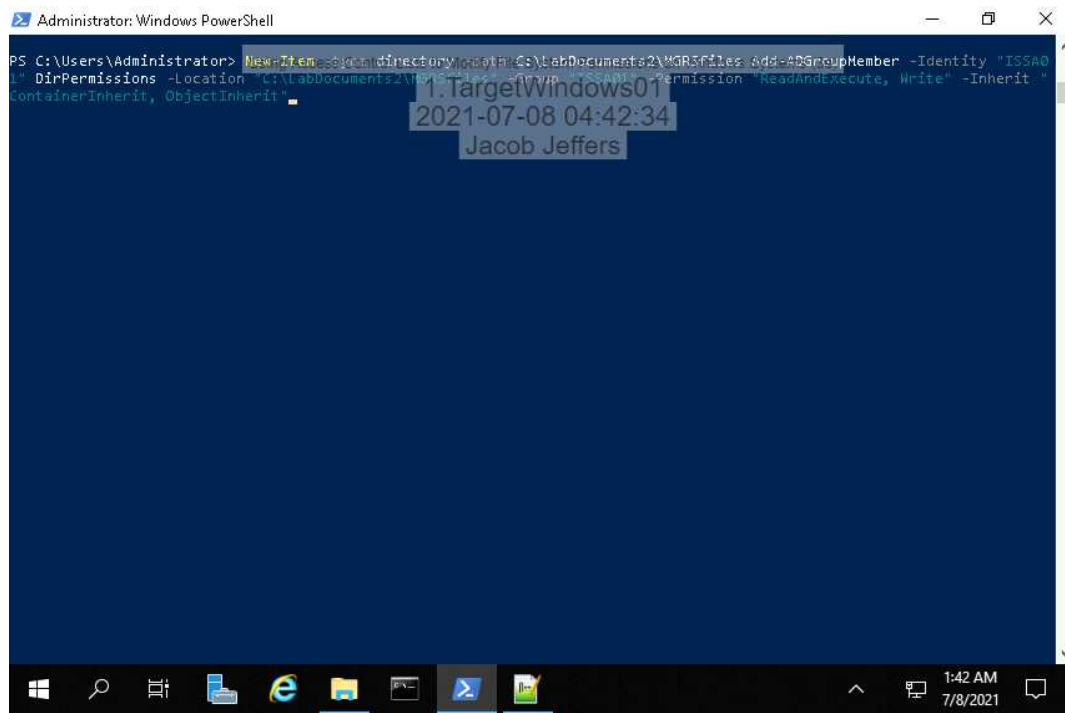
Part 3: Modify Permissions using a Script

2. Make a screen capture showing the current contents of the TargetWindows01 C: drive.

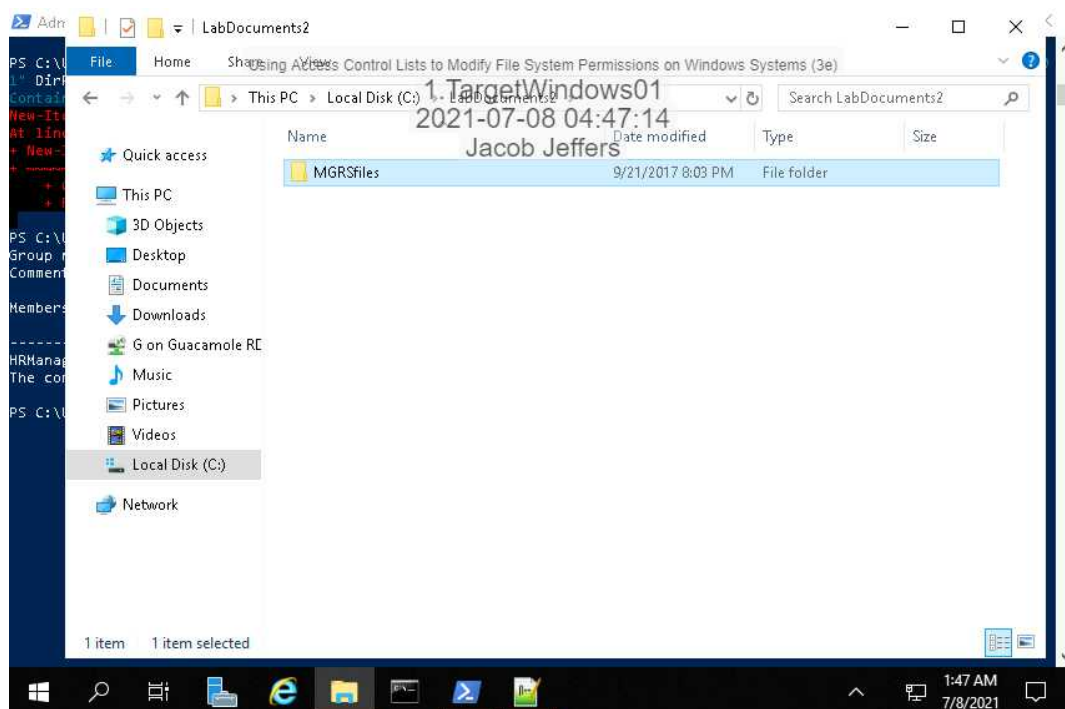


Part 4: Create Directories using a Script

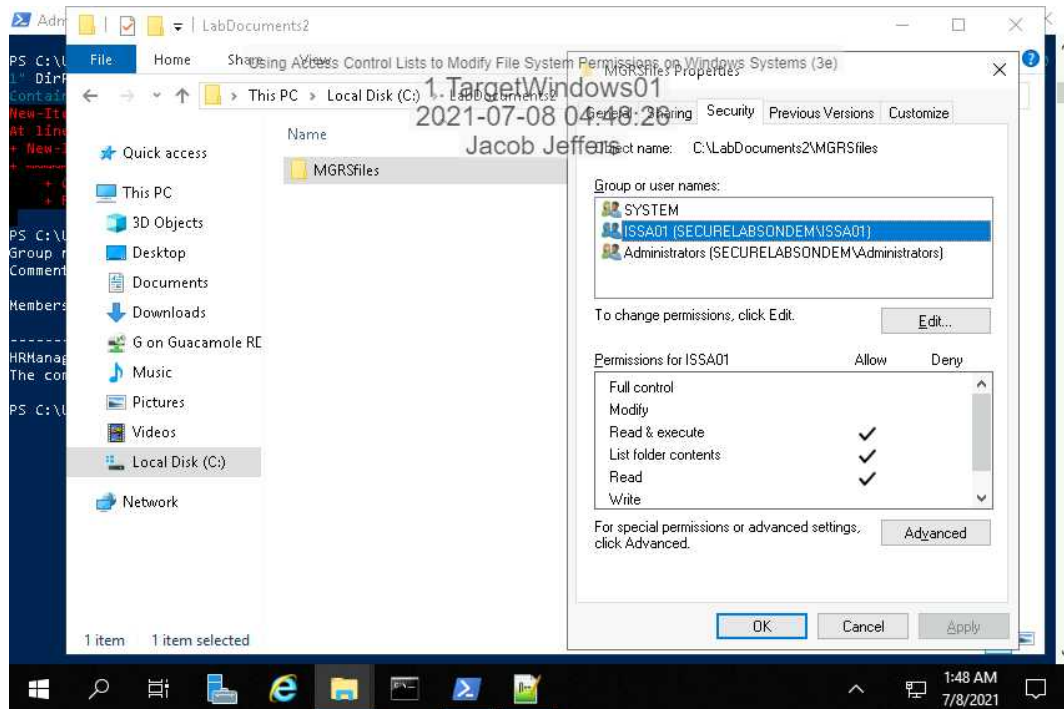
3. Make a screen capture showing the modifications to the final part of the script.



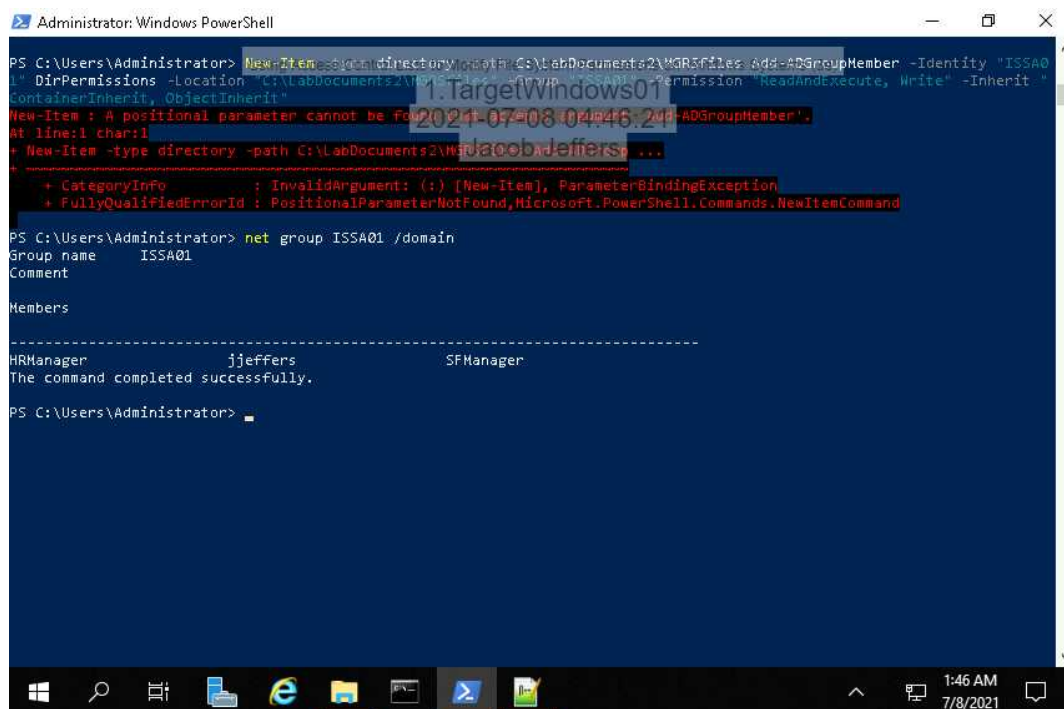
10. Make a screen capture showing the contents of the new LabDocuments2 directory.



12. Make a screen capture showing the permissions for the ISSA01 security group.



15. Make a screen capture showing the members of the ISSA01 security group.



Section 3: Challenge and Analysis

Part 1: Analysis and Discussion

Explain how the principle of least privilege can be used in a corporate setting to protect corporate resources.

The principle of least privilege, for example, could prevent entry-level accountants from investigating details that only a senior accountant might have. This is useful for protecting resources in a corporate resources, and it provides confidentiality.

Part 2: Tools and Commands

Research ACLs on the Internet and **identify** the permissions required to rename existing files.

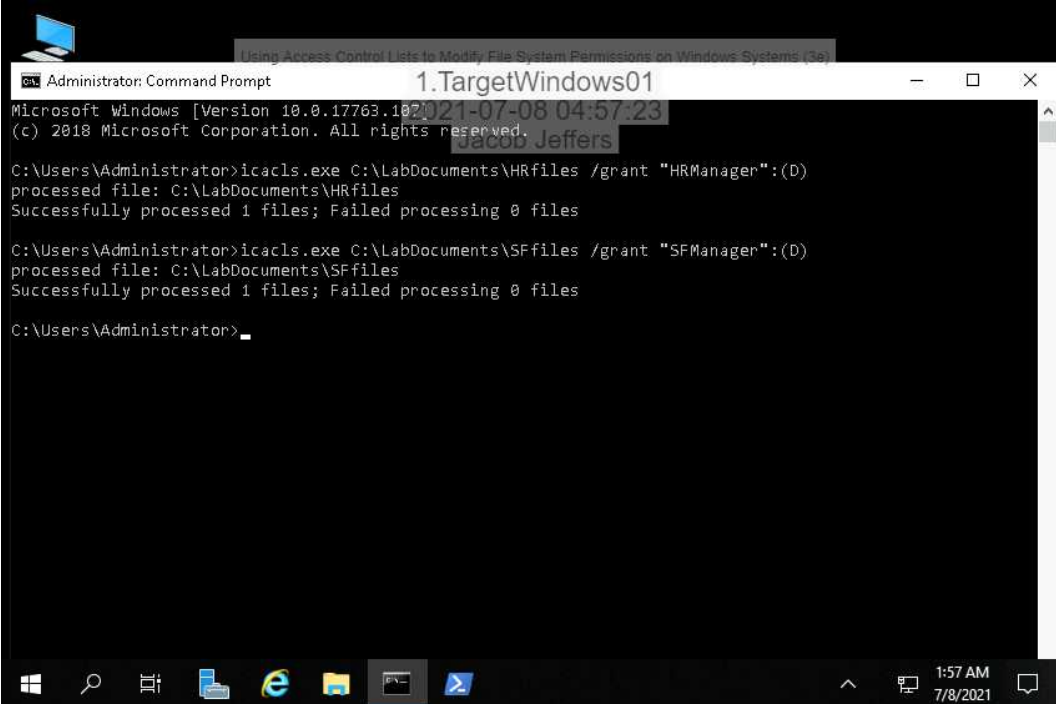
ACLs can be renamed using the WDAC command.

Part 3: Challenge Exercise

Describe the choices you've made.

I have granted the HR manager and the SF manager delete privileges using the command -
*icacls.exe C:\LabDocuments\HRfiles /grant "HRManager":(D) and *icacls C:\LabDocuments\SFfiles
/grant "SFManager":(D).

Make a screen capture showing your **successfully executed icacis commands**.



The screenshot shows a Windows Command Prompt window titled "Administrator: Command Prompt". The window displays the following text:

```
Microsoft Windows [Version 10.0.17763.107] (c) 2018 Microsoft Corporation. All rights reserved.  
C:\Users\Administrator>icacis.exe C:\LabDocuments\HRfiles /grant "HRManager":(D)  
processed file: C:\LabDocuments\HRfiles  
Successfully processed 1 files; Failed processing 0 files  
  
C:\Users\Administrator>icacis.exe C:\LabDocuments\SFfiles /grant "SFManager":(D)  
processed file: C:\LabDocuments\SFfiles  
Successfully processed 1 files; Failed processing 0 files  
  
C:\Users\Administrator>
```

The taskbar at the bottom shows the Windows logo, search icon, task view icon, and several application icons. The system clock in the bottom right corner indicates 1:57 AM on 7/8/2021.