

Student:	Email:
Bradley Adams	badams10@my.athens.edu

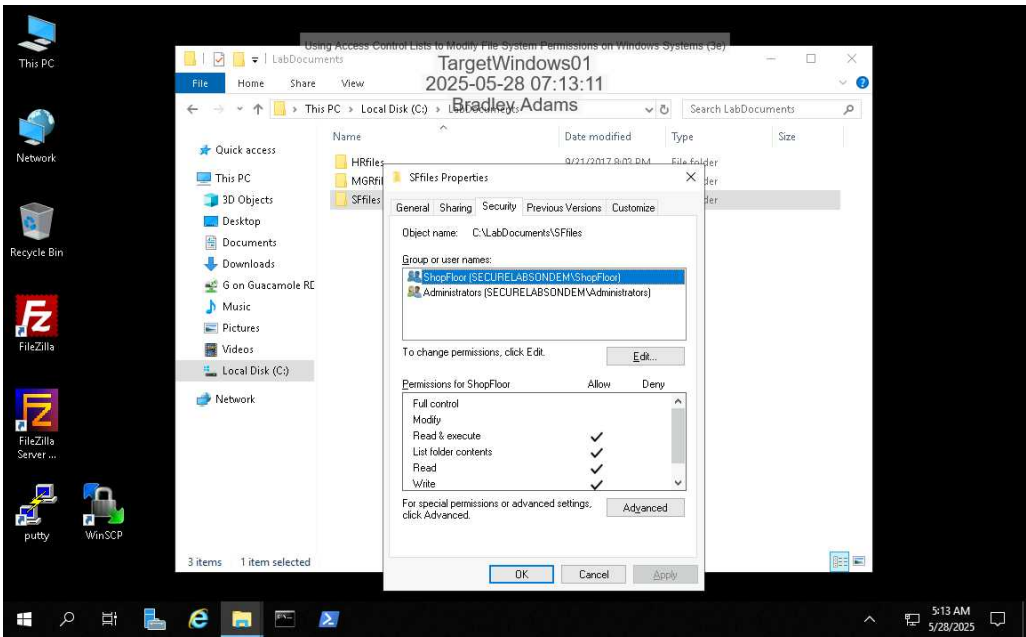
Time on Task:	Progress:
9 hours, 18 minutes	100%

Report Generated: Wednesday, May 28, 2025 at 1:00 PM

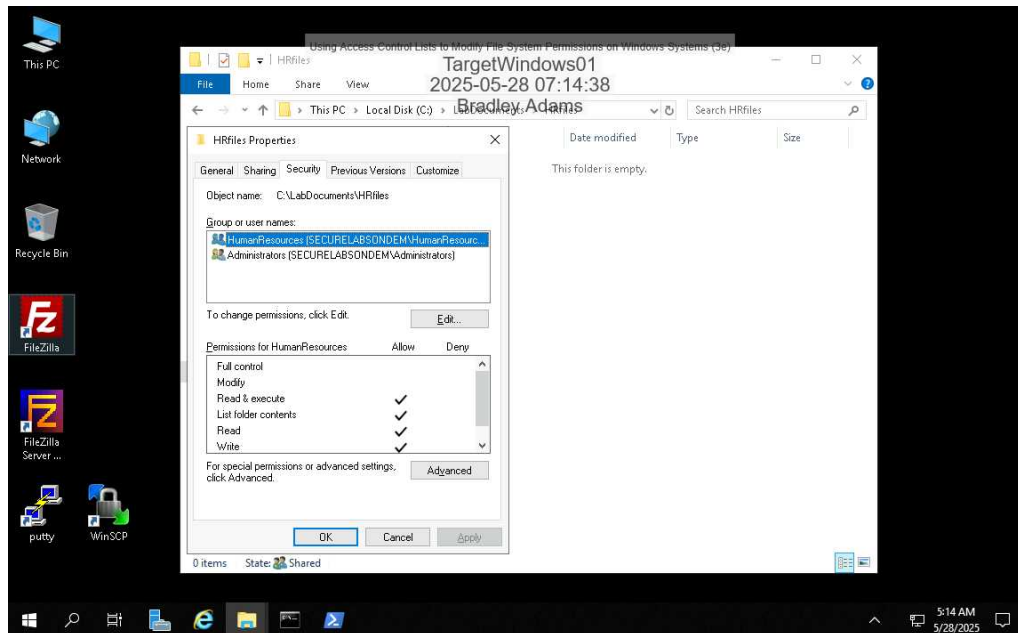
Section 1: Hands-On Demonstration

Part 1: View Existing ACLs on a Windows System

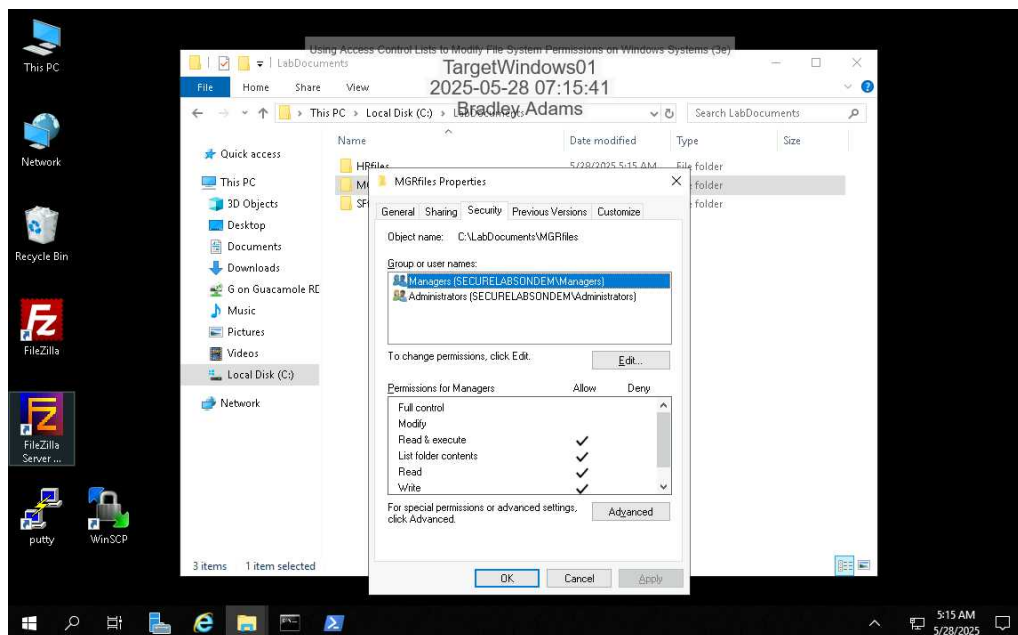
- 5. Make a screen capture showing the current permissions for the SFfiles folder.



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 Icacls.exe

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

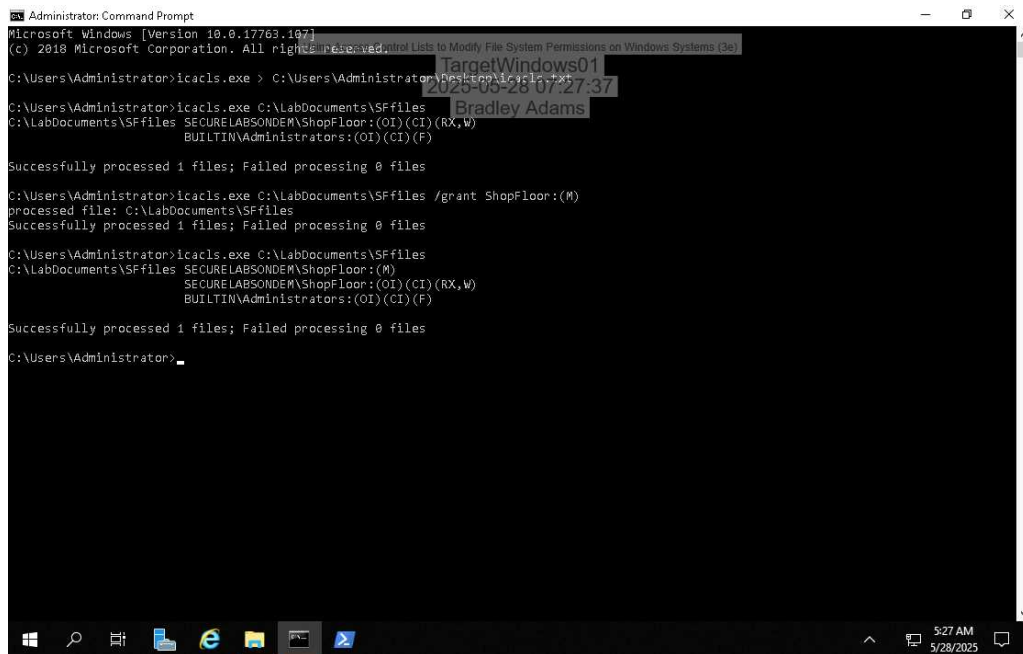
Yes

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.

The results are correct.

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



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

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

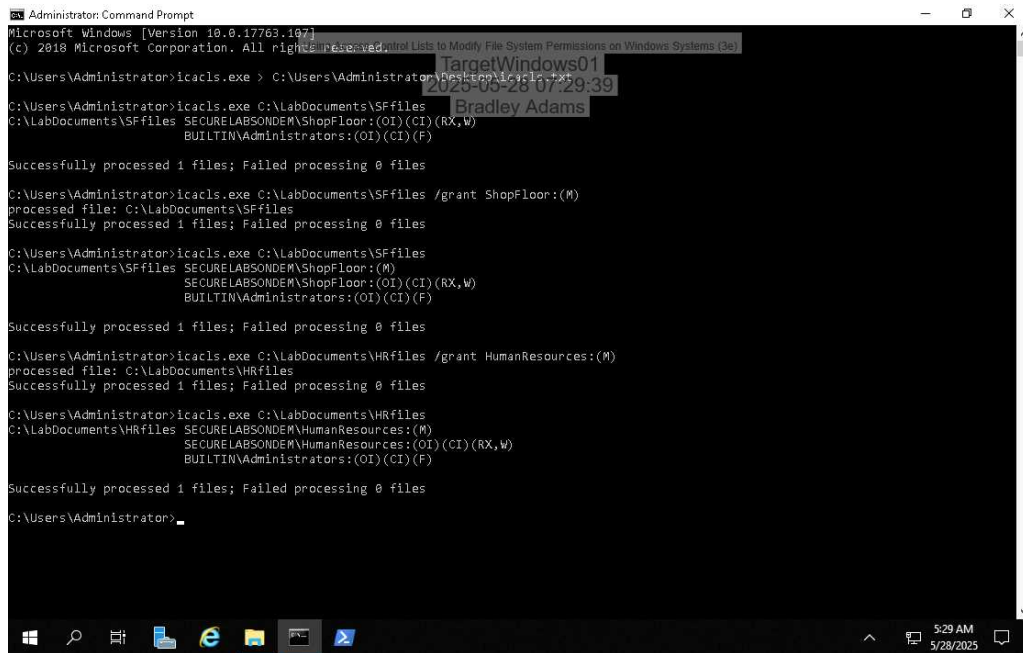
Successfully processed 1 files; Failed processing 0 files

C:\Users\Administrator>icacls.exe C:\LabDocuments\SFfiles /grant ShopFloor:(M)
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
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

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

Successfully processed 1 files; Failed processing 0 files

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

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

Successfully processed 1 files; Failed processing 0 files

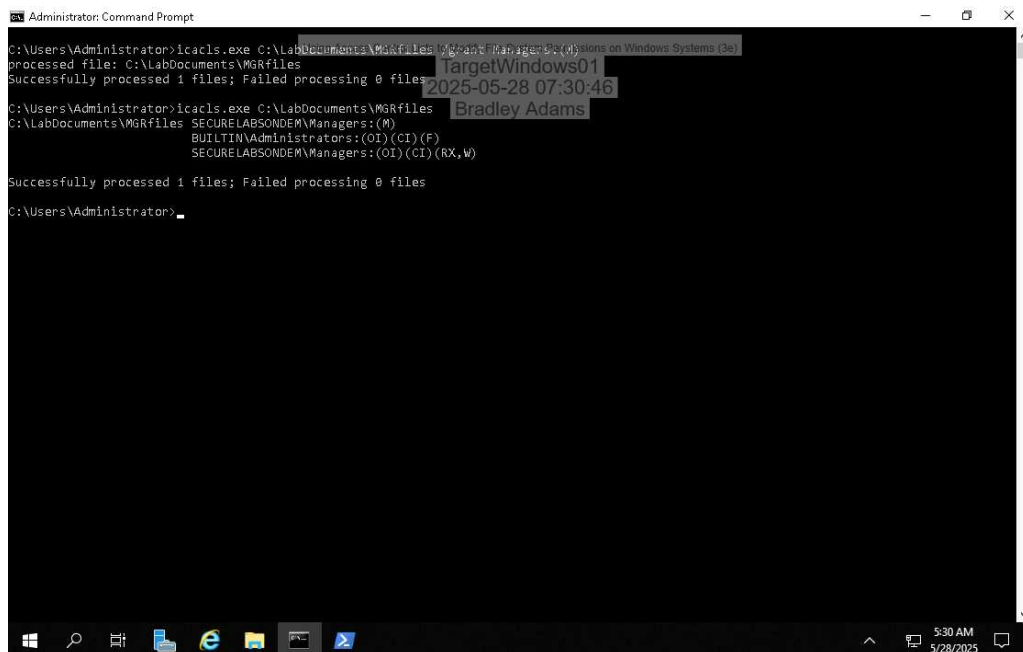
C:\Users\Administrator>icaccls.exe C:\LabDocuments\HRfiles /grant HumanResources:(M)
processed file: C:\LabDocuments\HRfiles
Successfully processed 1 files; Failed processing 0 files

C:\Users\Administrator>icaccls.exe C:\LabDocuments\HRfiles
C:\LabDocuments\HRfiles SECURITYLABSONDEM\HumanResources:(M)
SECURITYLABSONDEM\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
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>icaccls.exe C:\LabDocuments\MGRfiles
processed file: C:\LabDocuments\MGRfiles
Successfully processed 1 files; Failed processing 0 files

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

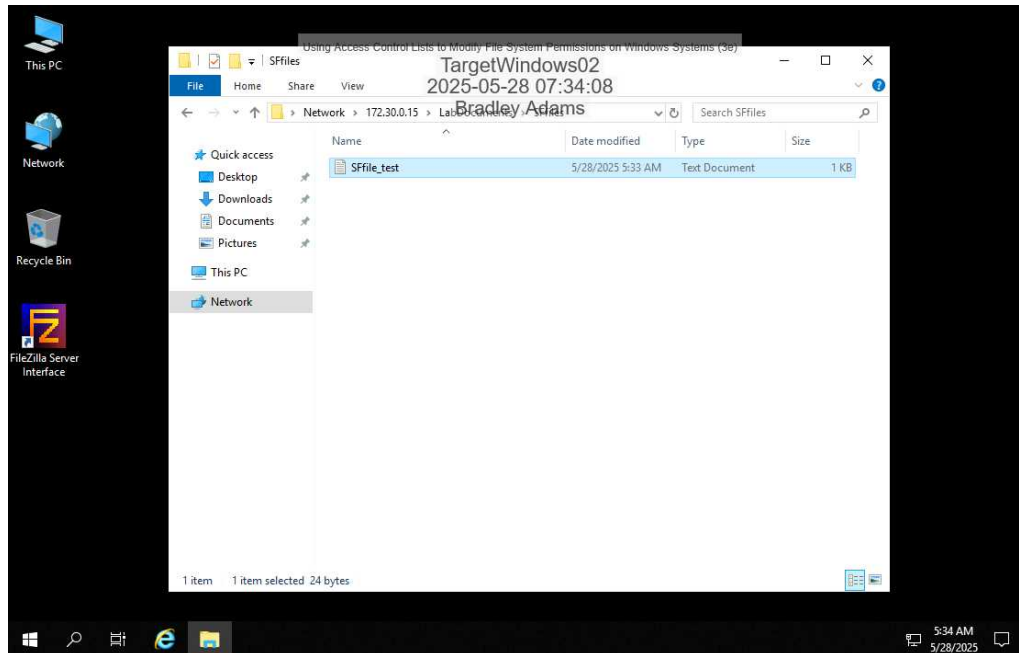
Successfully processed 1 files; Failed processing 0 files

C:\Users\Administrator>
```

Part 3: Validate ACL Settings

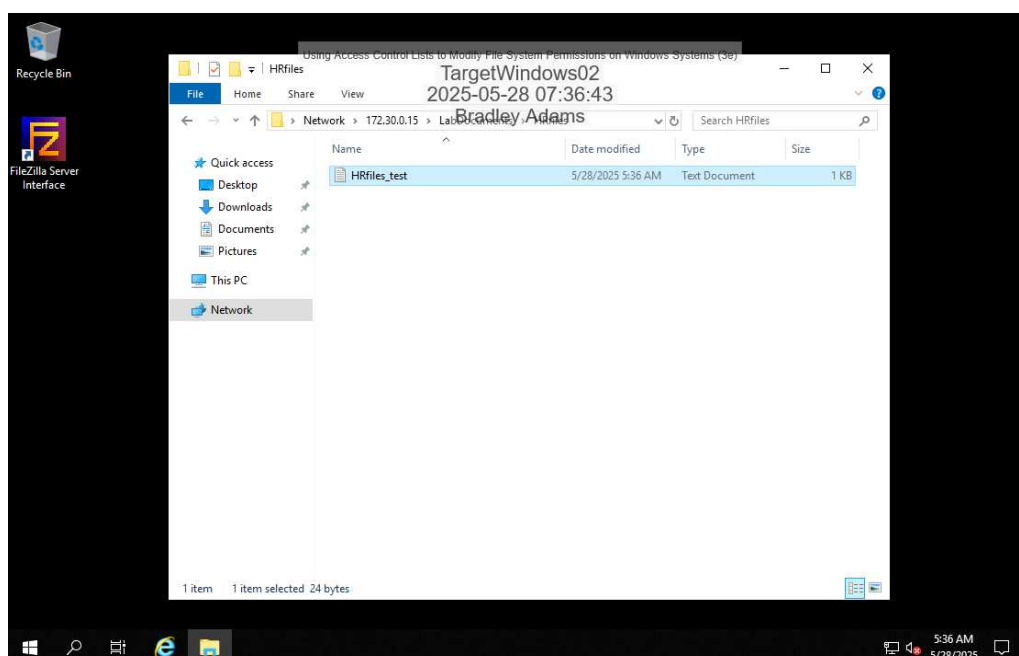
14. **Make a screen capture** showing the **modified text file** in the **SFfiles** folder.

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



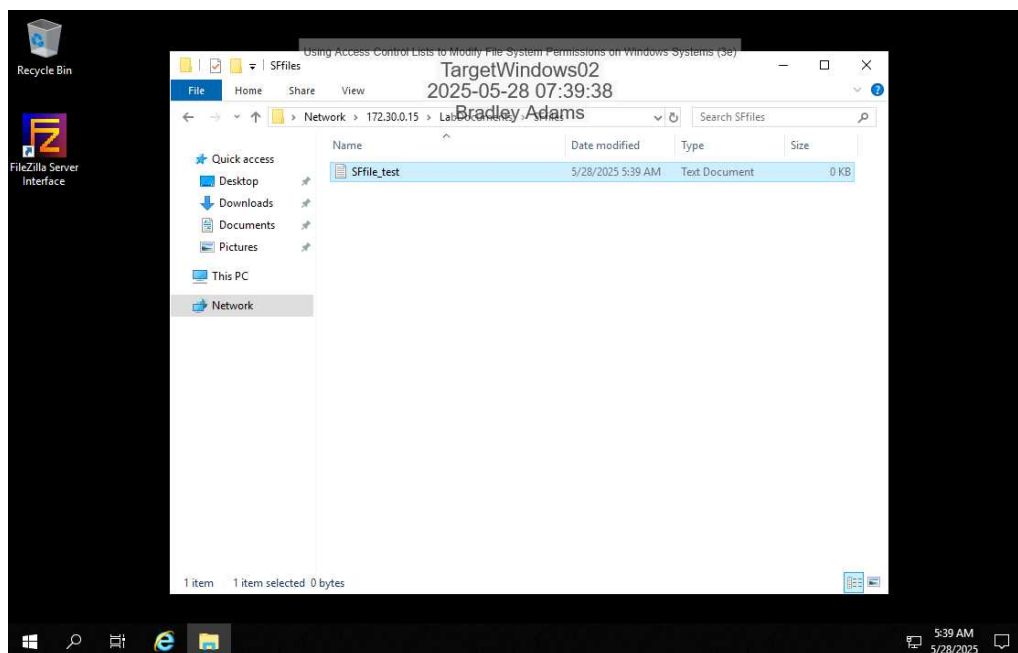
17. **Make a screen capture** showing the **modified text file** in the **HRfiles** folder.

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



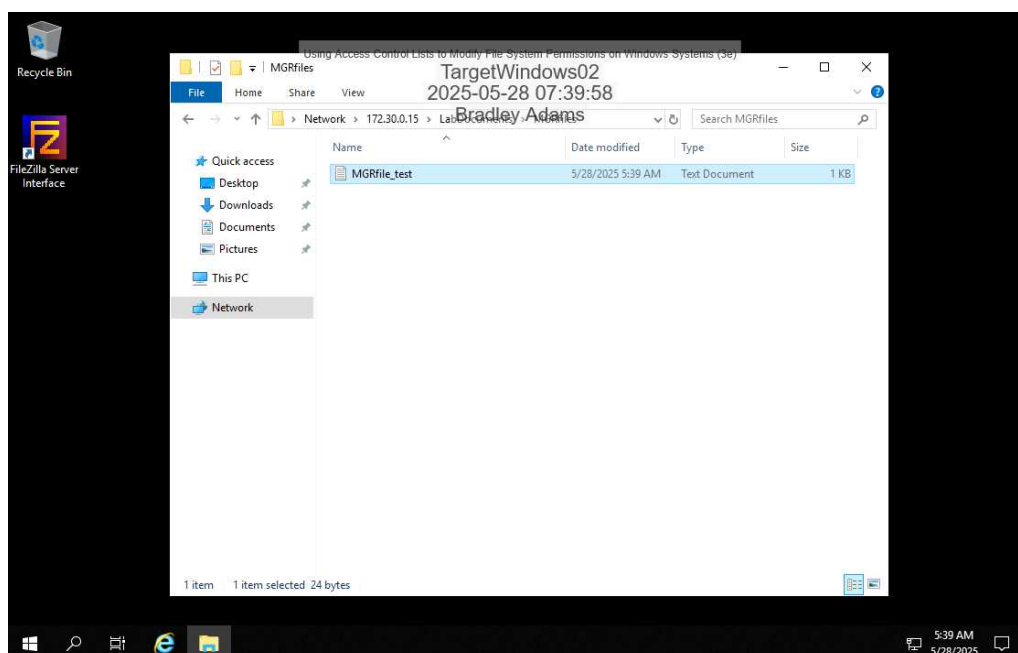
20. **Make a screen capture** showing the **re-modified text file** in the **SFiles** folder.

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.

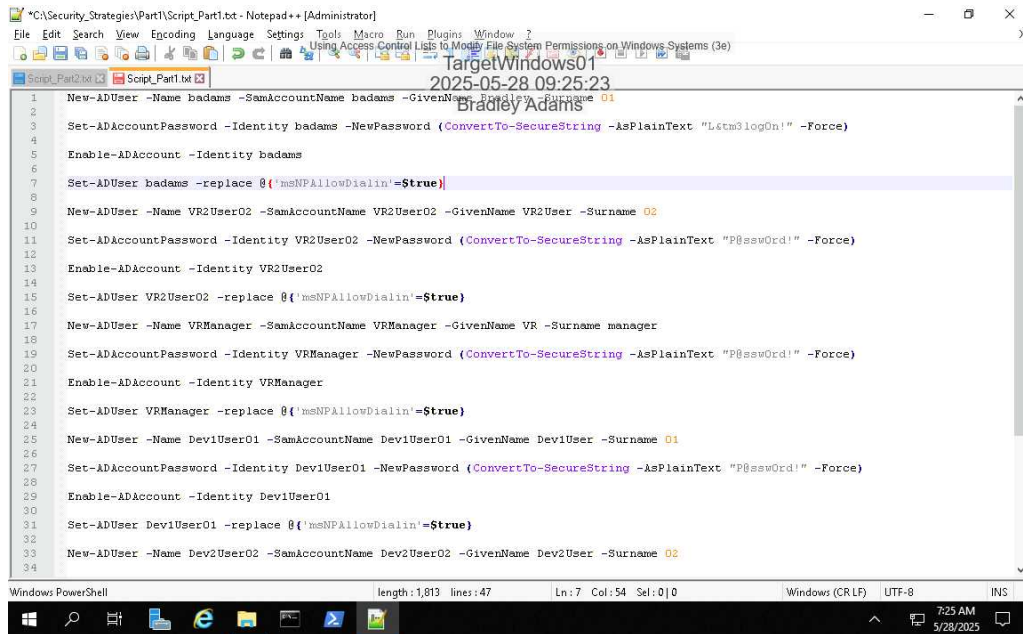
The modified file will show a 1 KB value in the Size column, indicating that text has been added to the file.



Section 2: Applied Learning

Part 1: Add a New User using a Script

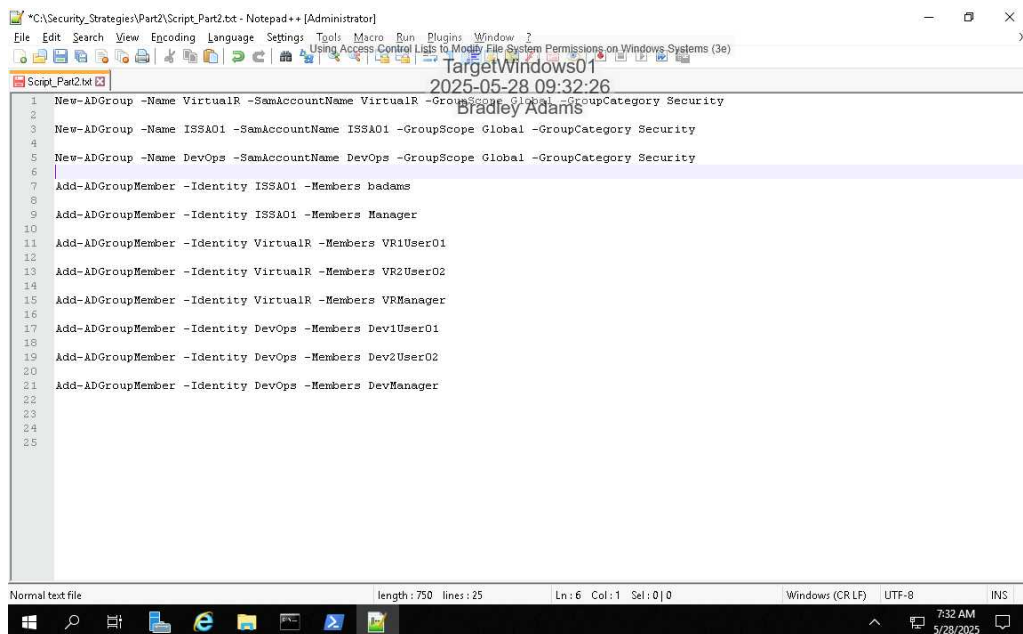
3. Make a screen capture showing the new user account in this script.



```
*C:\Security_Strategies\Part1\Script_Part1.txt - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
Script_Part1.txt
1 New-ADUser -Name badams -SamAccountName badams -GivenName Bradley -Surname 01
2
3 Set-ADAccountPassword -Identity badams -NewPassword (ConvertTo-SecureString -AsPlainText "L&tm3logOn!" -Force)
4
5 Enable-ADAccount -Identity badams
6
7 Set-ADUser badams -replace @{'msNPAllowDialin'=$true}
8
9 New-ADUser -Name VR2User02 -SamAccountName VR2User02 -GivenName VR2User -Surname 02
10
11 Set-ADAccountPassword -Identity VR2User02 -NewPassword (ConvertTo-SecureString -AsPlainText "P@sswOrd!" -Force)
12
13 Enable-ADAccount -Identity VR2User02
14
15 Set-ADUser VR2User02 -replace @{'msNPAllowDialin'=$true}
16
17 New-ADUser -Name VRManager -SamAccountName VRManager -GivenName VR -Surname manager
18
19 Set-ADAccountPassword -Identity VRManager -NewPassword (ConvertTo-SecureString -AsPlainText "P@sswOrd!" -Force)
20
21 Enable-ADAccount -Identity VRManager
22
23 Set-ADUser VRManager -replace @{'msNPAllowDialin'=$true}
24
25 New-ADUser -Name Dev1User01 -SamAccountName Dev1User01 -GivenName Dev1User -Surname 01
26
27 Set-ADAccountPassword -Identity Dev1User01 -NewPassword (ConvertTo-SecureString -AsPlainText "P@sswOrd!" -Force)
28
29 Enable-ADAccount -Identity Dev1User01
30
31 Set-ADUser Dev1User01 -replace @{'msNPAllowDialin'=$true}
32
33 New-ADUser -Name Dev2User02 -SamAccountName Dev2User02 -GivenName Dev2User -Surname 02
34
Windows PowerShell length: 1,813 lines: 47 Ln: 7 Col: 54 Sel: 0|0 Windows (CR LF) UTF-8 INS 7:25 AM 5/28/2025
```

Part 2: Add a New Group using a Script

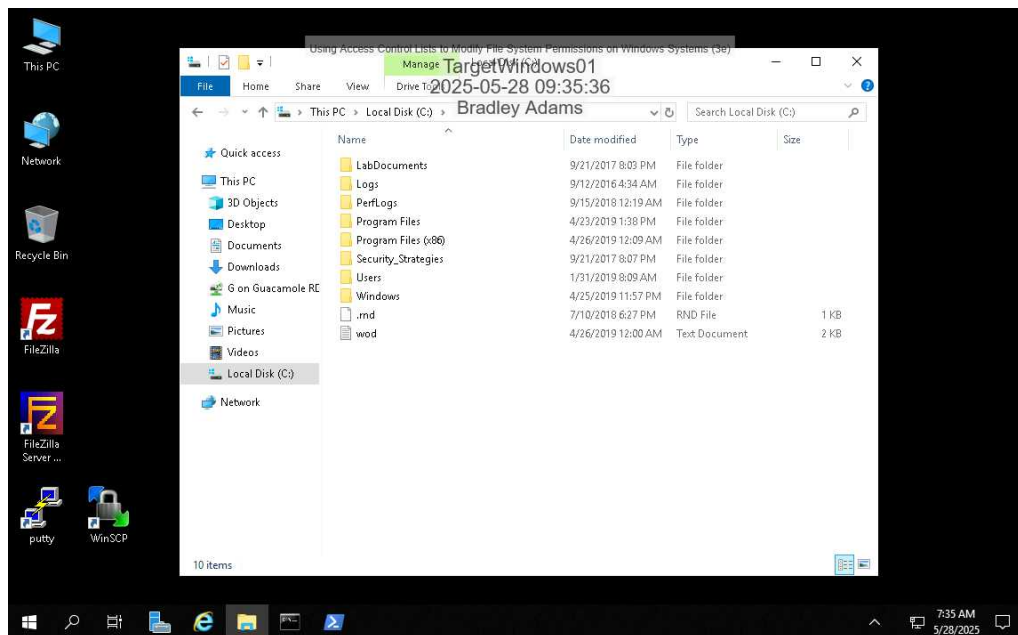
5. Make a screen capture showing the modifications you made to the script.



```
*C:\Security_Strategies\Part2\Script_Part2.txt - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
Script_Part2.txt
1 New-ADGroup -Name VirtualR -SamAccountName VirtualR -GroupScope Global -GroupCategory Security
2
3 New-ADGroup -Name ISSA01 -SamAccountName ISSA01 -GroupScope Global -GroupCategory Security
4
5 New-ADGroup -Name DevOps -SamAccountName DevOps -GroupScope Global -GroupCategory Security
6
7 Add-ADGroupMember -Identity ISSA01 -Members badams
8
9 Add-ADGroupMember -Identity ISSA01 -Members Manager
10
11 Add-ADGroupMember -Identity VirtualR -Members VR1User01
12
13 Add-ADGroupMember -Identity VirtualR -Members VR2User02
14
15 Add-ADGroupMember -Identity VirtualR -Members VRManager
16
17 Add-ADGroupMember -Identity DevOps -Members Dev1User01
18
19 Add-ADGroupMember -Identity DevOps -Members Dev2User02
20
21 Add-ADGroupMember -Identity DevOps -Members DevManager
22
23
24
25
Normal text file length: 750 lines: 25 Ln: 6 Col: 1 Sel: 0|0 Windows (CR LF) UTF-8 INS 7:32 AM 5/28/2025
```

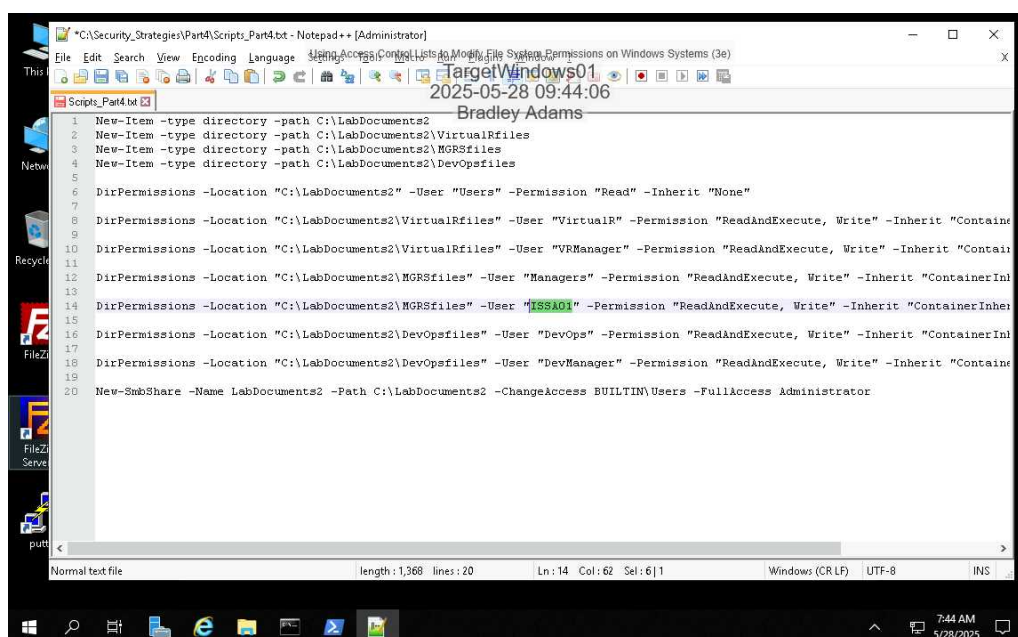

Part 3: Modify Permissions using a Script

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

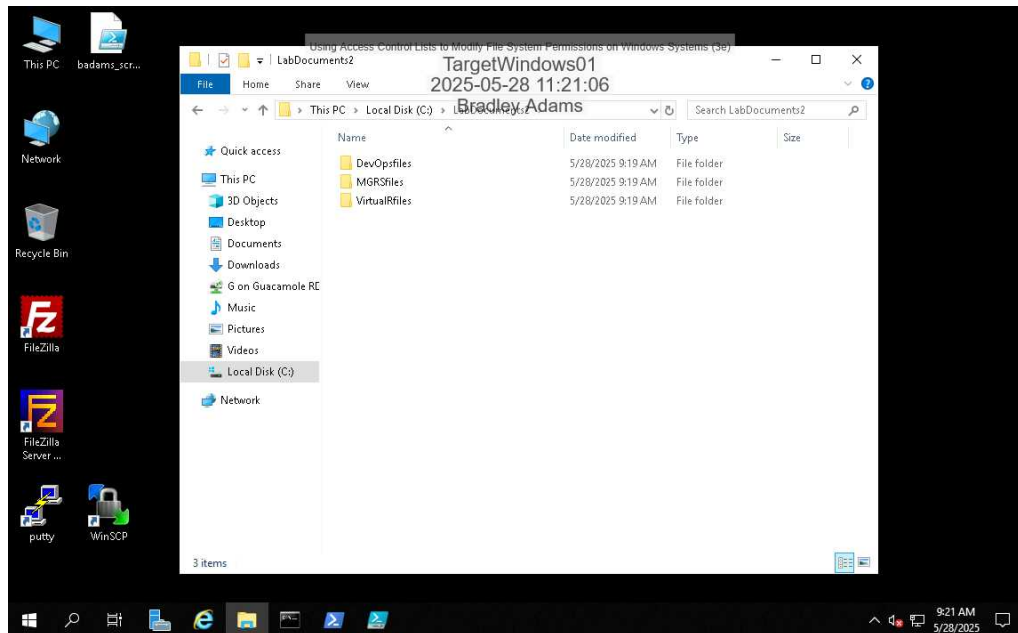


Part 4: Create Directories using a Script

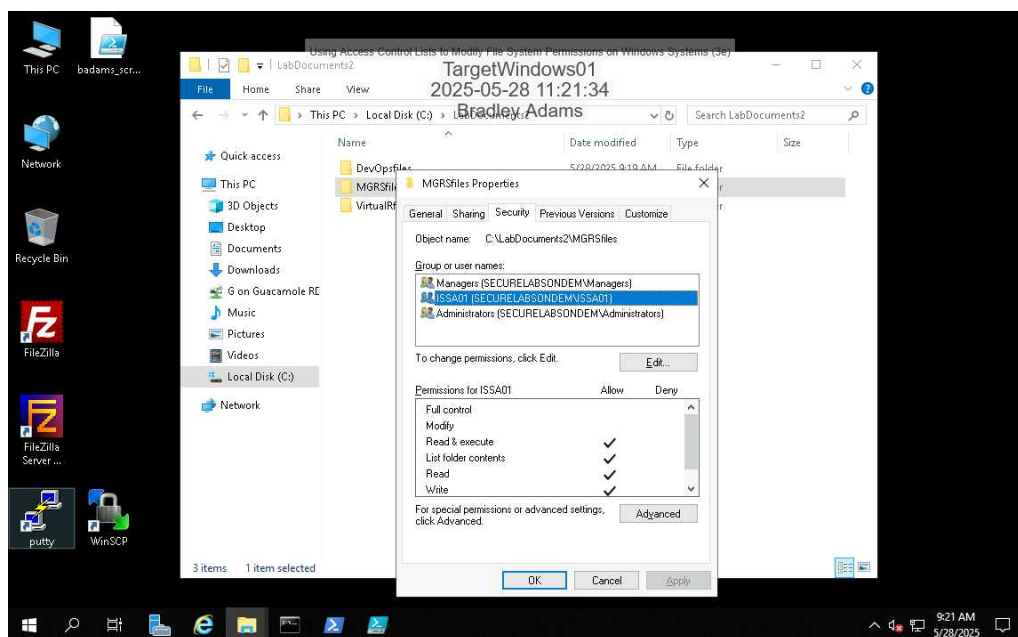
3. Make a screen capture showing the modifications to the final part of the script.



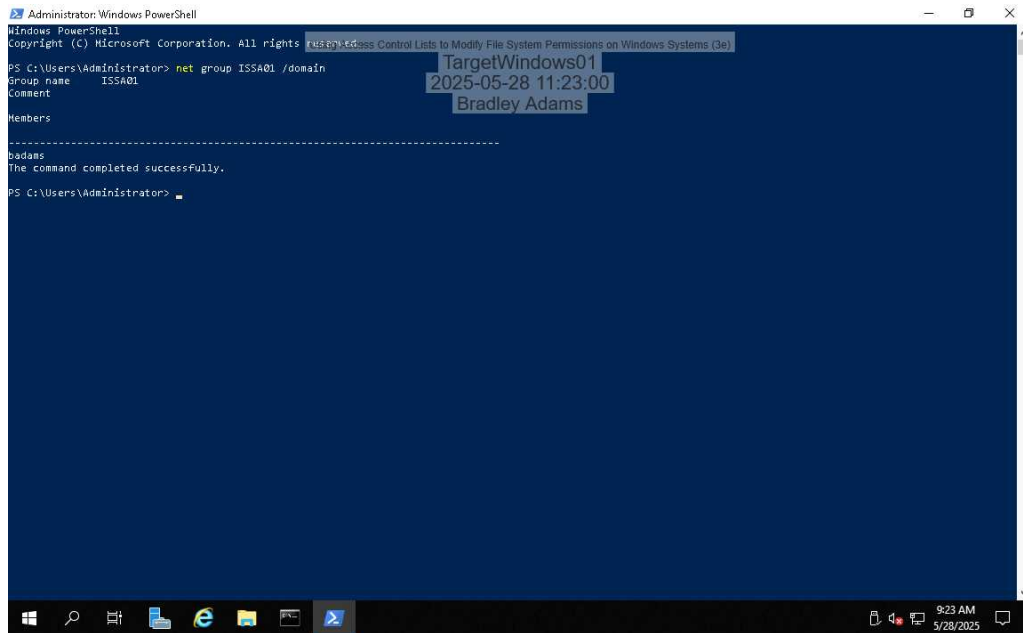
10. Make a screen capture showing the contents of the new LabDocuments2 directory.



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.



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
PS C:\Users\Administrator> net group ISSA01 /domain
Group name      ISSA01
Comment
Members
-----
badams
The command completed successfully.
PS C:\Users\Administrator>
```

The screenshot shows a Windows PowerShell window titled "Administrator: Windows PowerShell". The command prompt shows the command `net group ISSA01 /domain` being executed. The output displays the group name as `ISSA01` and the comment as `badams`. The command completed successfully. The window also shows the Windows taskbar at the bottom with the date and time as 9:23 AM on 5/28/2025.

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 is a foundational security concept that limits user and system access to only what is necessary to perform their job functions. This technique minimizes potential damage from accidents, errors, or malicious activity. It reduces the attack surface by limiting users' and applications' rights so that those rights are not excessive, which could be exploitable if compromised. By assigning permissions based on roles, organizations secure users within their responsibilities. This strategy also helps isolate breaches to limit an attacker's access. Applying the least privilege principle to service accounts, administrative tools, and software processes helps mitigate lateral movement within a network.

Part 2: Tools and Commands

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

Delete to delete the original file name.

Write allows the user to create a new file or modify an existing file. Write is necessary to give a file a new name.

Read allows the user to read the file properties during the renaming process.

Modify includes all the permissions listed above and allows users to rename files.

Part 3: Challenge Exercise

Describe the choices you've made.

I added the Delete permission for the Managers group to the MGRfiles folder. I used the command, `icacls.exe C:\LabDocuments\MGRfiles /grant Managers:(D)`

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

