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

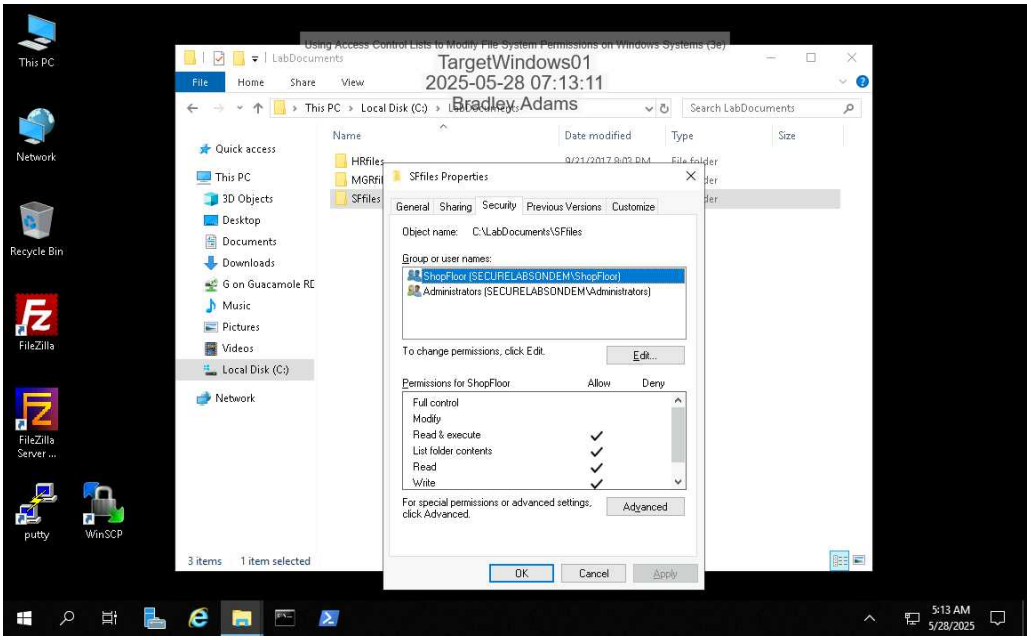
Time on Task:	Progress:
9 hours, 18 minutes	100%

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

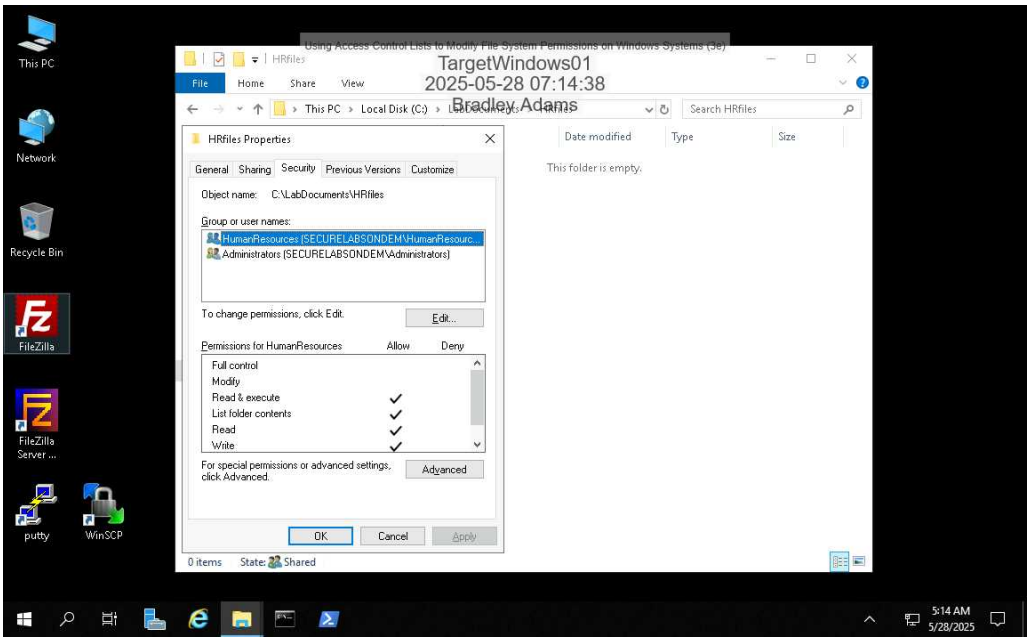
Section 1: Hands-On Demonstration

Part 1: View Existing ACLs on a Windows System

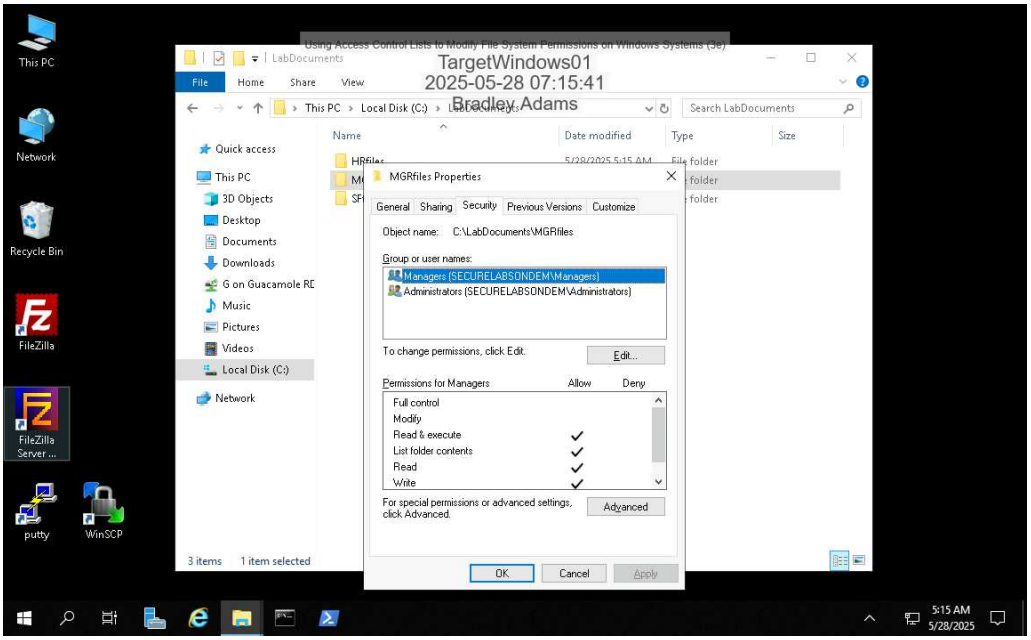
5. **Make a screen capture** showing the **current permissions for the SFfiles folder**.



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

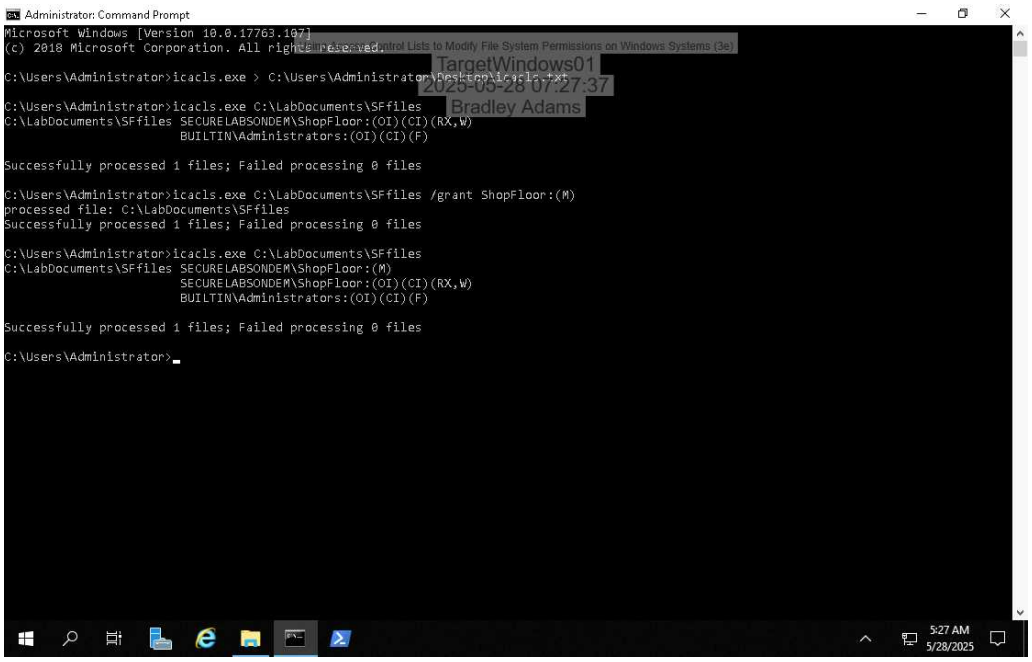
8. **Compare the results** of the icacls.exe command with the ACLs you reviewed in Part 1 of this lab. Do they match?

Yes

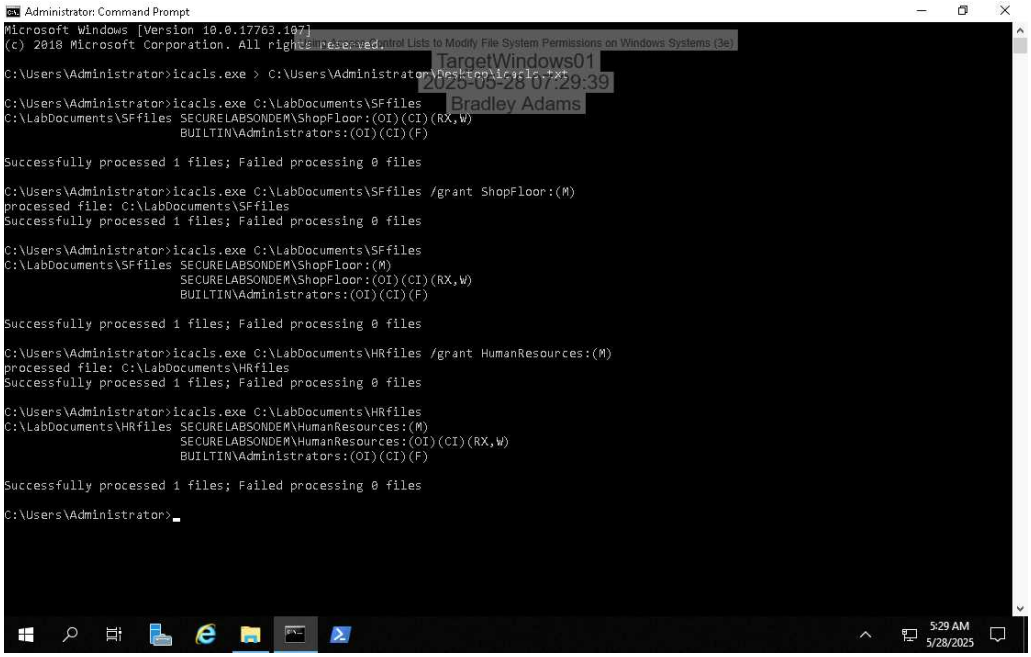
11. **Compare the new results** of this command with the results from step 7.
You should notice that there is now a new line item for SECURELABSONDEM\ShopFloor. The grant command creates a new line item for any principal with permissions added through icacls.exe; technically, icacls.exe adds “special” permissions, which are visible by clicking the Advanced button in the folder Properties dialog box.

The results are correct.

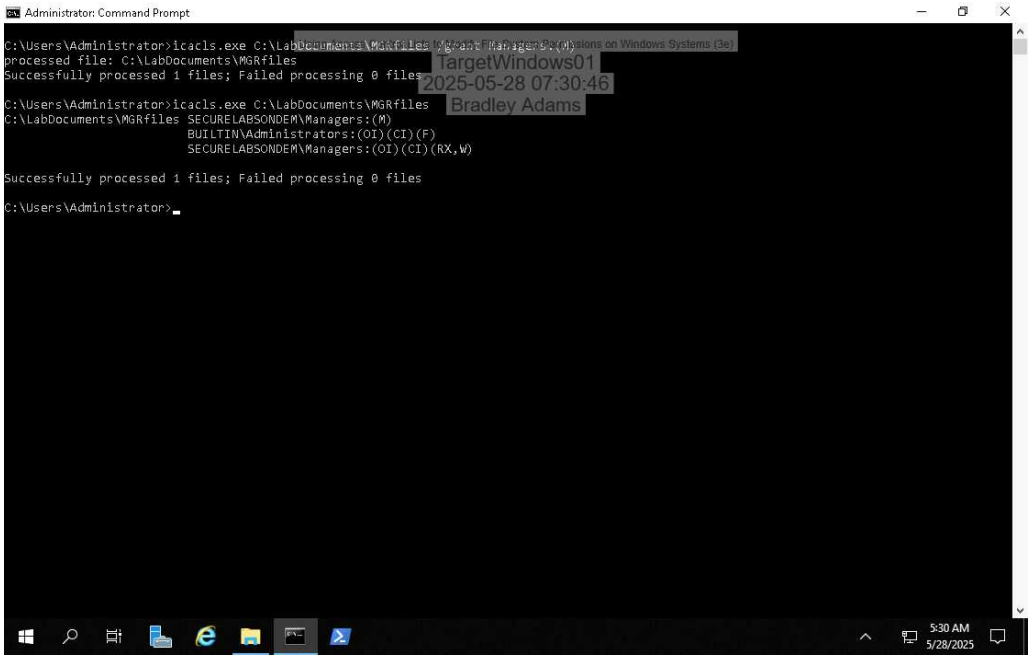
12. **Make a screen capture** showing the **changes you made to the SFfiles folder permissions**.



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



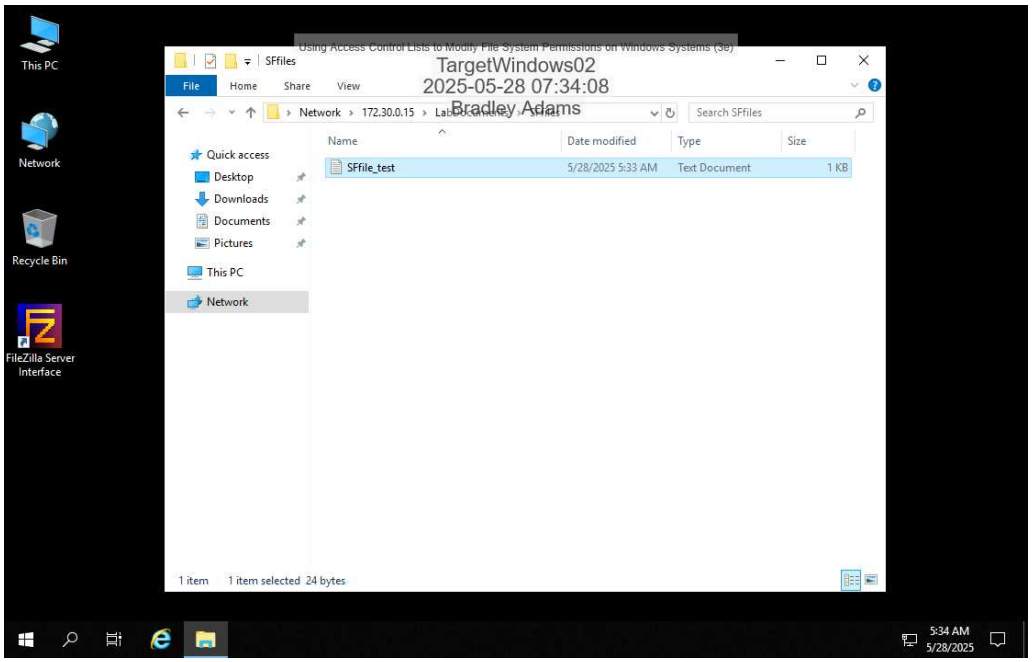
16. **Make a screen capture** showing the **changes you made to the MGRfiles folder permissions**.



Part 3: Validate ACL Settings

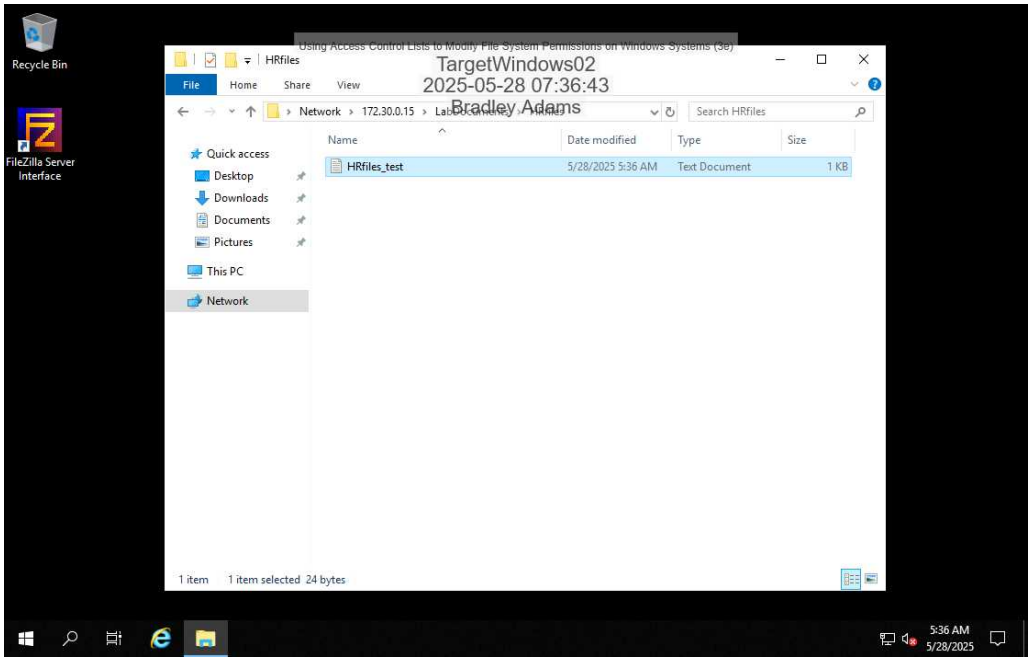
14. **Make a screen capture** showing the **modified text file in the SFfiles folder**.

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



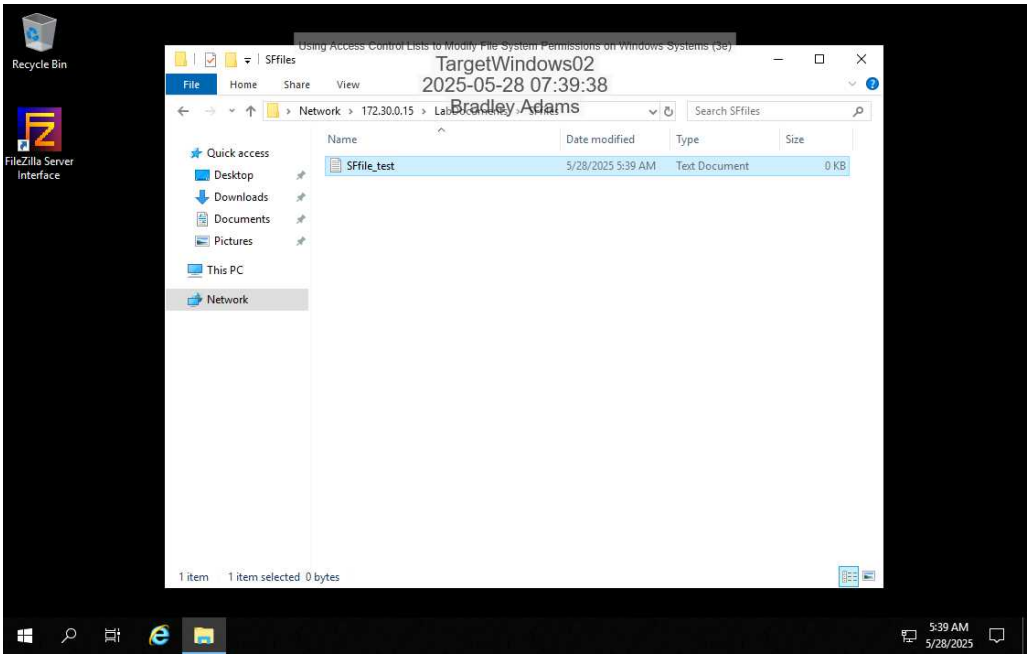
17. **Make a screen capture** showing the **modified text file in the HRfiles folder**.

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



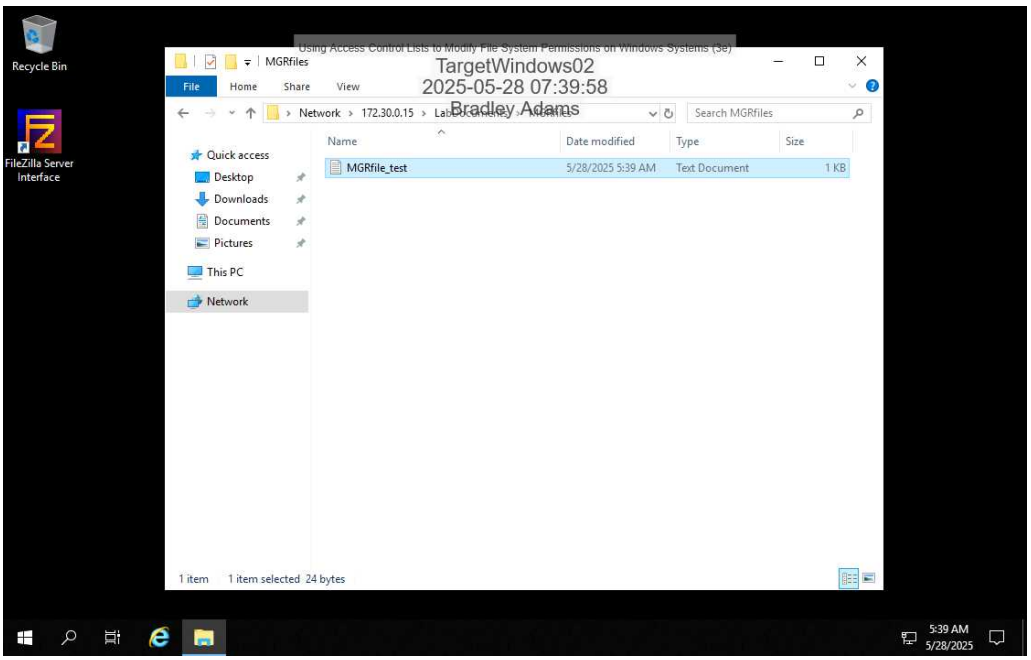
20. **Make a screen capture** showing the **re-modified text file in the SFfiles folder**.

    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**.

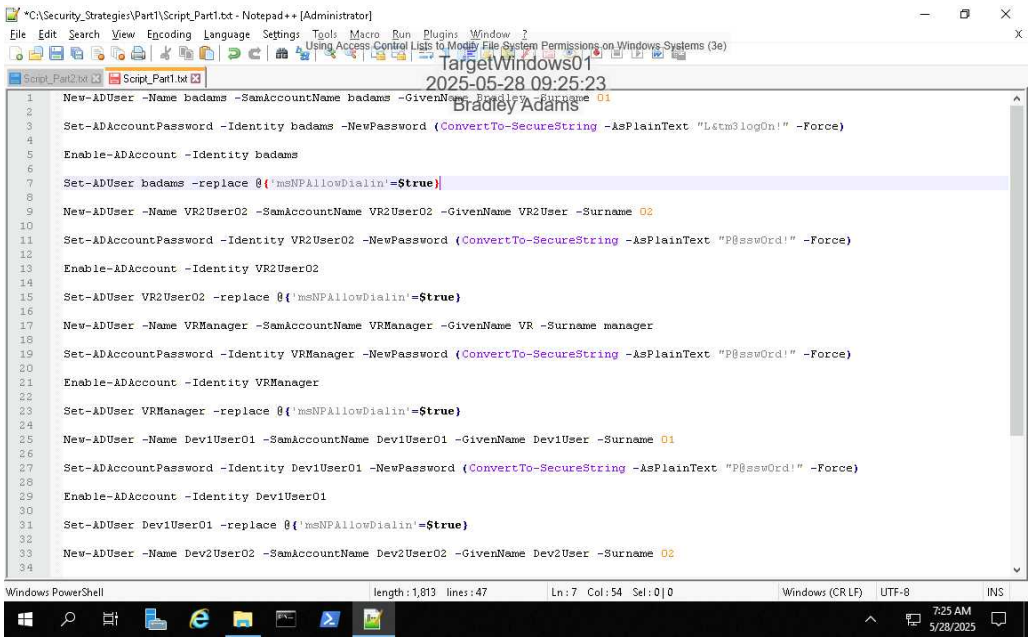
    The modified file will show a 1 KB value in the Size column, indicating that text has been added to the file.



Section 2: Applied Learning

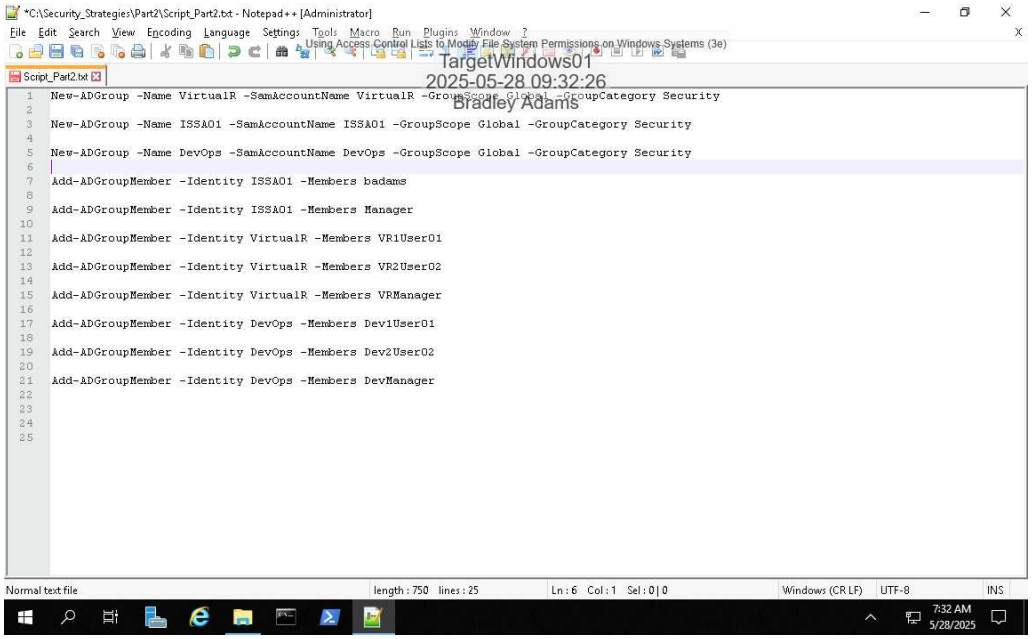
Part 1: Add a New User using a Script

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



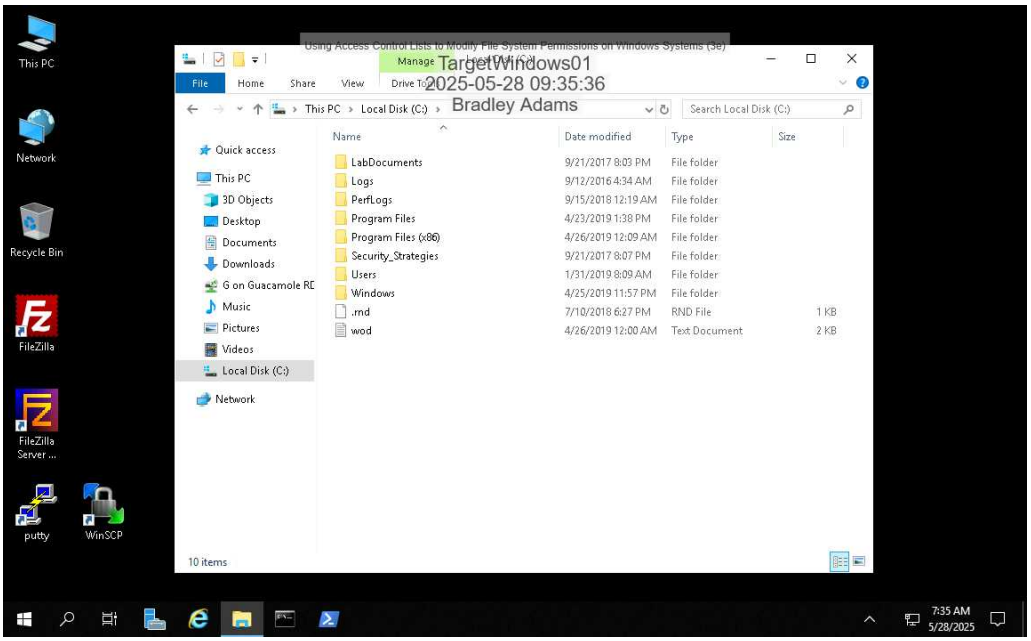
Part 2: Add a New Group using a Script

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



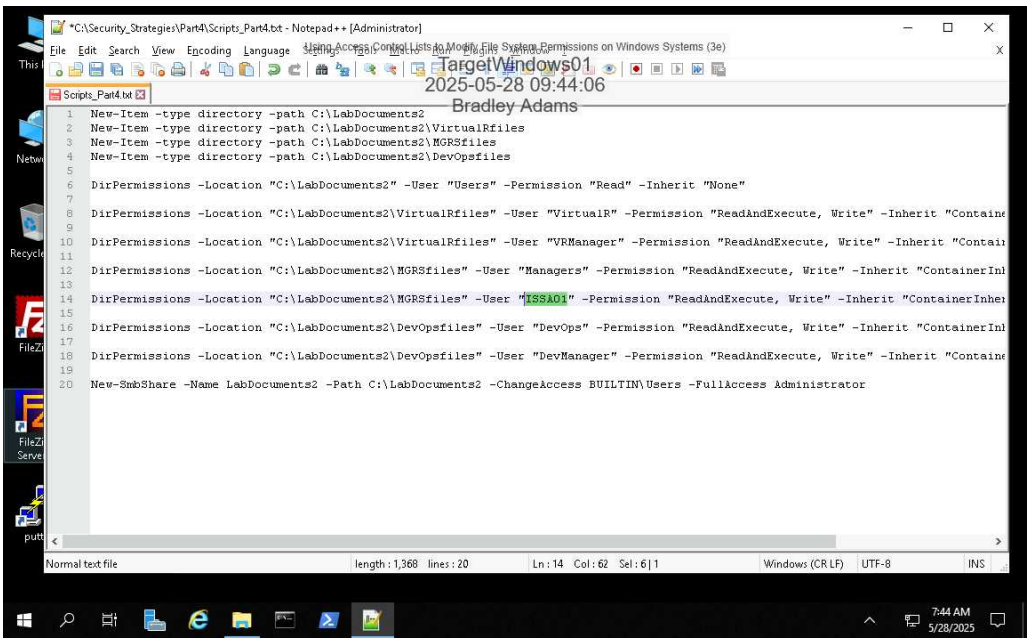
Part 3: Modify Permissions using a Script

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

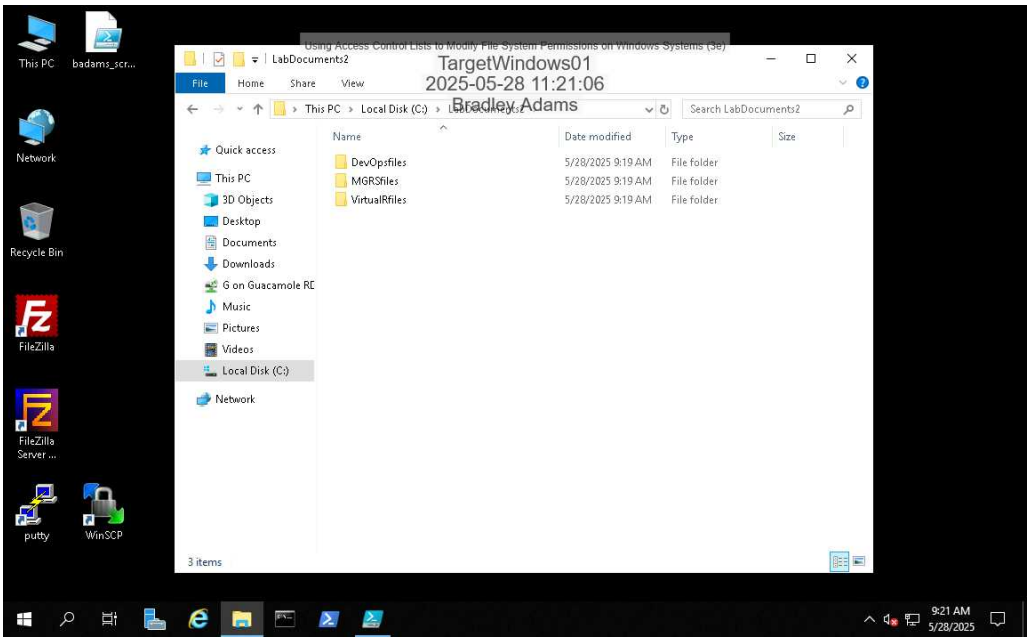


Part 4: Create Directories using a Script

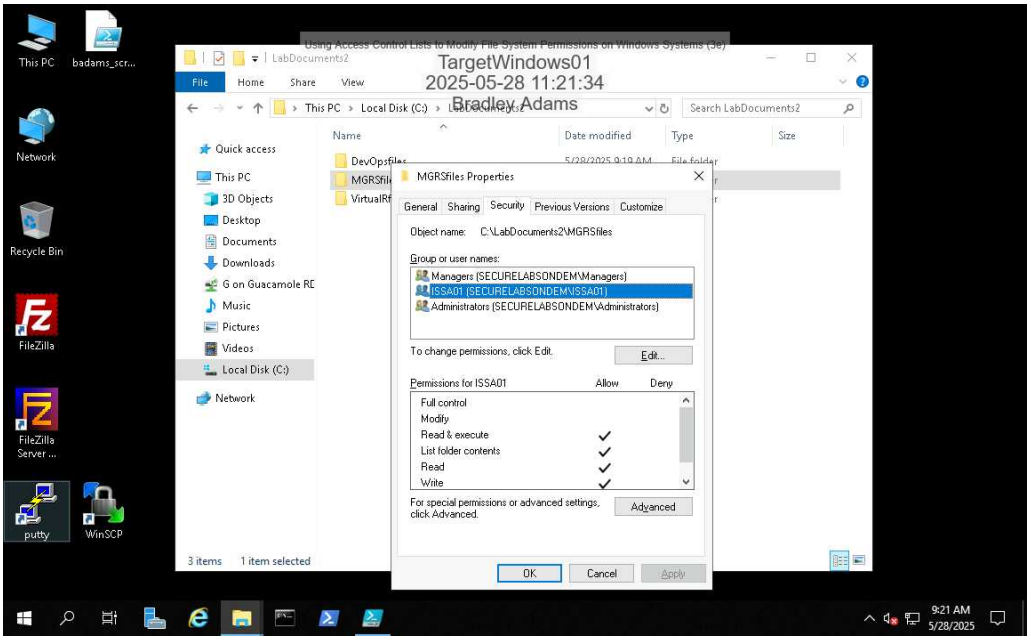
3. **Make a screen capture** showing the **modifications to the final part of the script**.



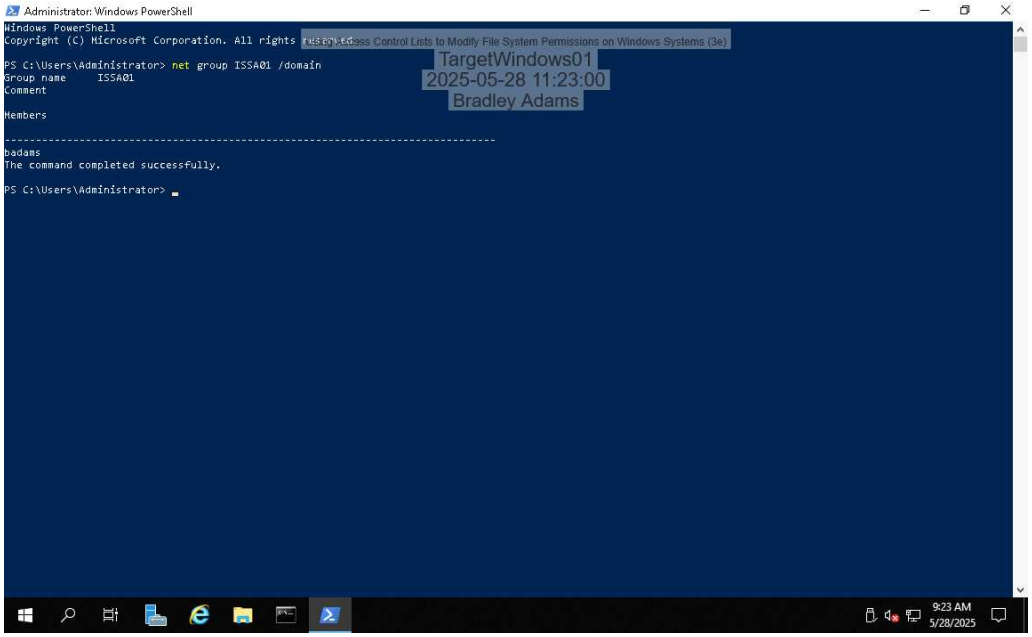
10. **Make a screen capture** showing the **contents of the new LabDocuments2 directory**.



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 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 icacls commands**.