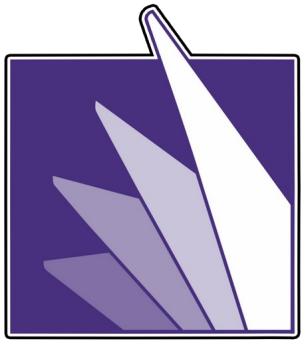


FLORIDA POLY®

[USER AUTHENTICATION & AUTHORIZATION]

CIS 4367.01 Computer Security, Fall 2025

Nickolas Diaz

[Xianping Wang]

Table of Contents

Contents

Abstract

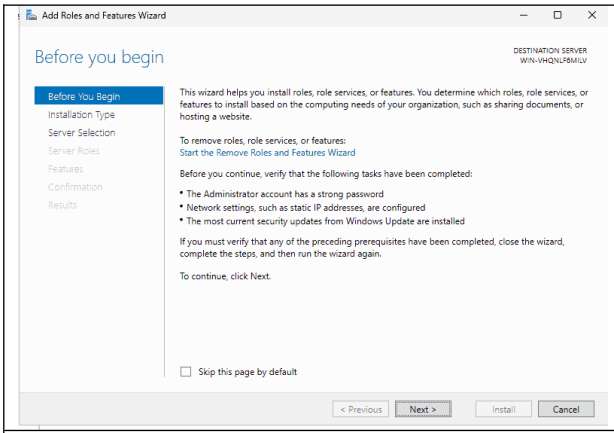
This lab will achieve setting up a domain using Active Directory on a Windows server 2025 virtual machine. It involves creating a domain service and 3 Organizational Units for each department with each department having groups such as chair, faculty and students. Each group will have their own permissions within the university such as viewing, reading or modifying files and directories within the university folder. I addition a complex password policy will be applied to the domain.

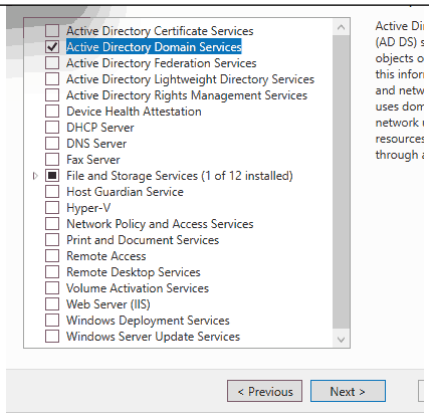
Tasks

Task 1: Installing and Configuring Active Director

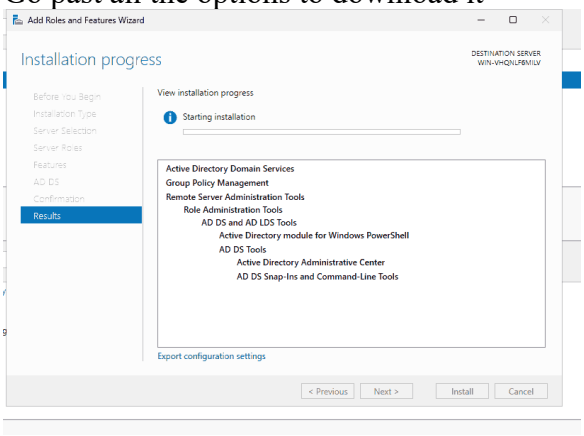
Install Active Directory Domain Service

After clicking the add roles and features from server manager, this pop-up apprears	On the instalation type press Active Diretory Domain Service

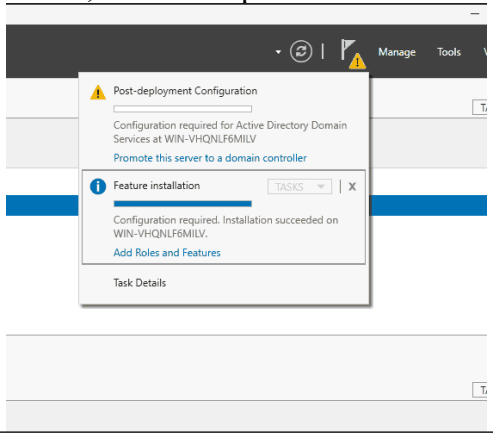




Go past all the options to download it

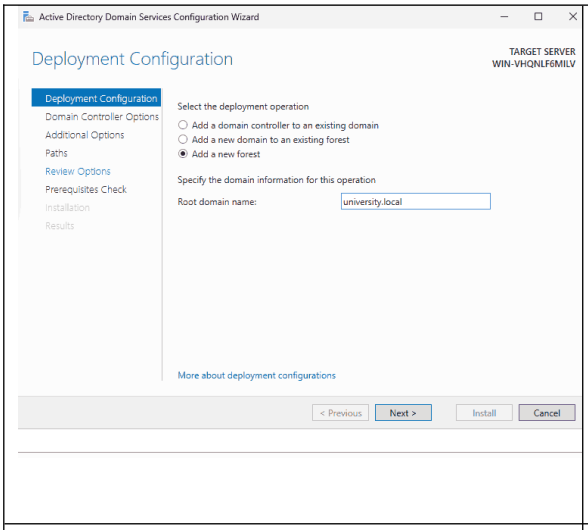


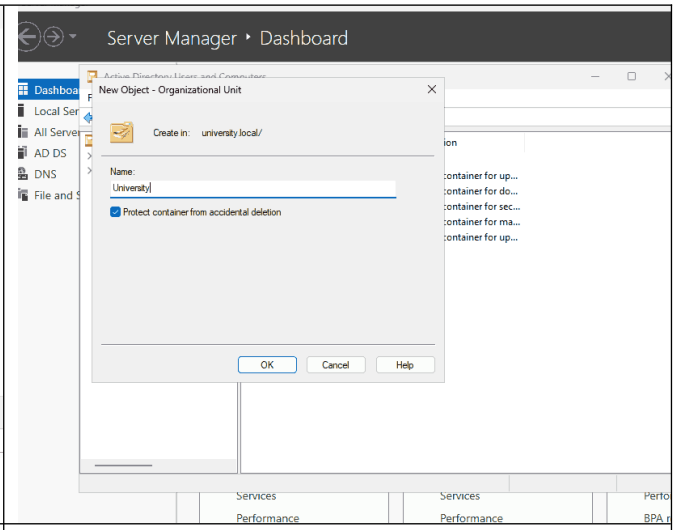
From here it will start downloading and restart, once done proceed to the next step



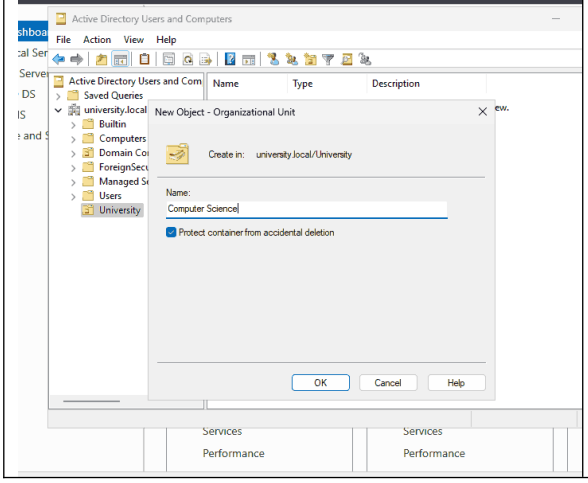
Configure Active Directory Users and Computers

Pop-up apprears after clicking Active Directory Users and Computers from the server manager. In addition I added the domain university.local	After the domain was created I created a organizational unit called University.

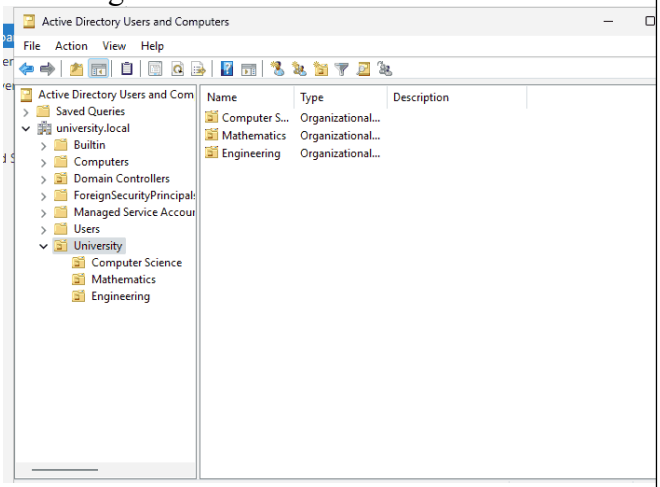




In the organizational unit I created three sub-OUs called Computer Science, Mathematics, and Engineering

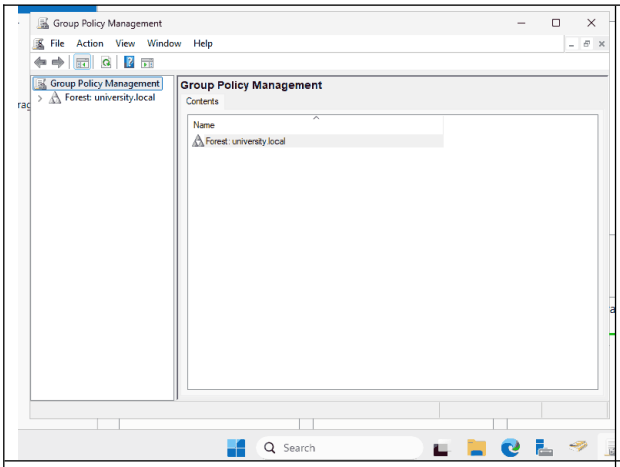


This is the tree view of the organisational unit, including sub Ous.

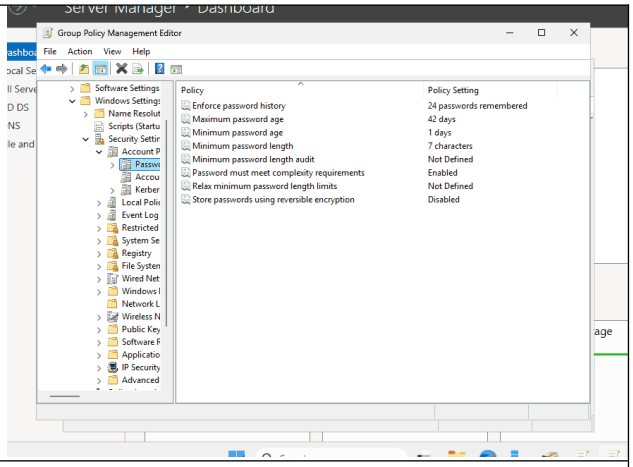


Task 2: Enable Complex Password Policy for All Users

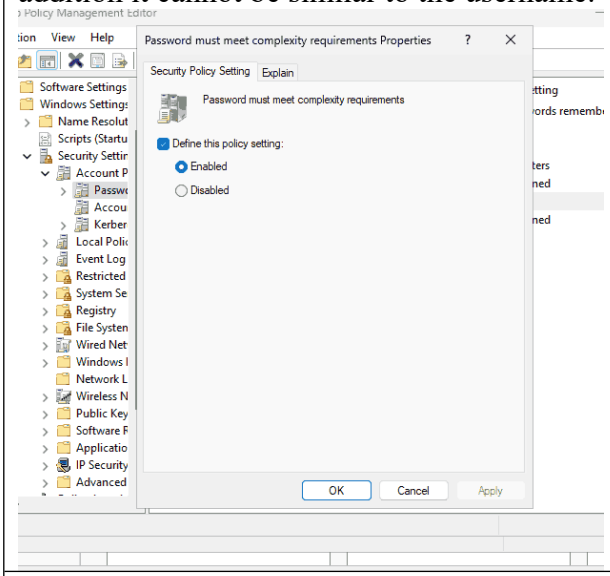
First I headed to Group Policy Management, I typed gpmc.msc in the terminal to open it.	From Group Policy Management > Forest > Domains > university.local > Computer Configuration > Polices > Windows Settings > Security Settings > Account Polices > Password Policy, is the location of the password complexity settings.



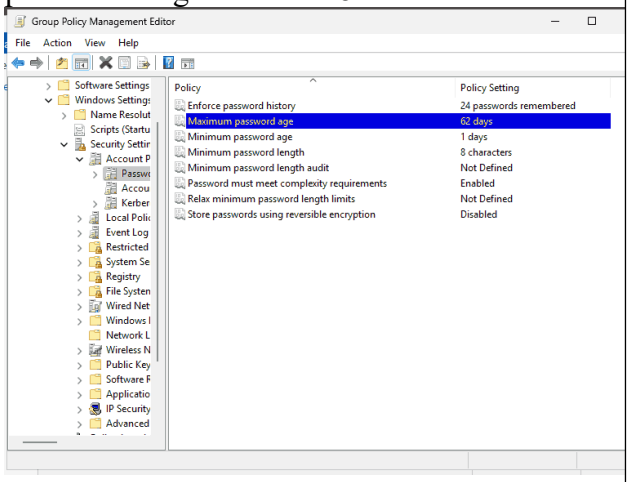
Clicking the password must meet complexity requirements, this pop-up shows, click enable to force the OU to have secure passwords, passwords have to use uppercase lowercase numbers Non-alphabetic characters and be up to 8 characters, in addition it cannot be similar to the username.



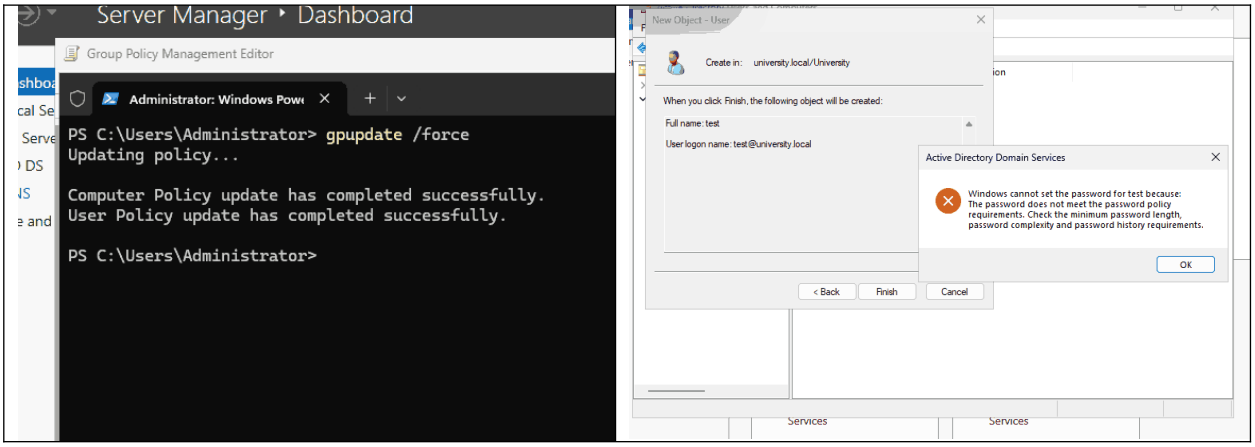
Other setting to modify are password history 24 previous passwords this means that you cannot reuse any passwords, Password age how long to get a new password and lastly password length which is 8



Lastly in order to make these policies take affect the command gpupdate /force is used.



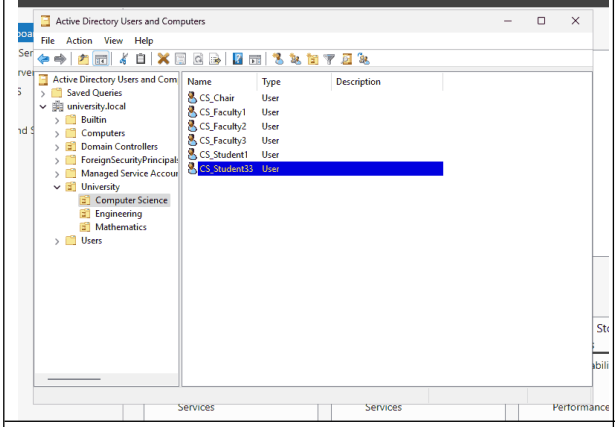
This is deminstrating the password complexity requirements in this case username and password were similar.



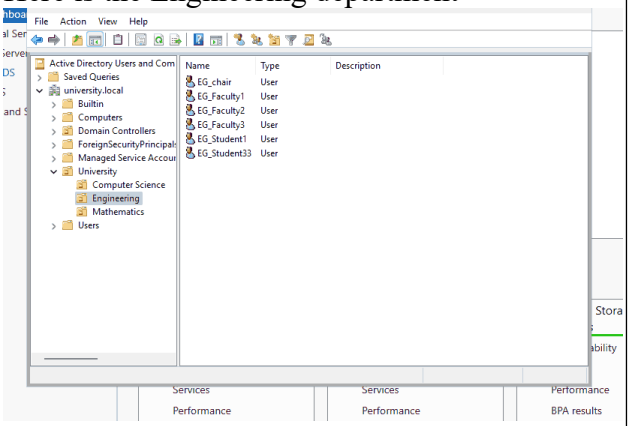
Task 3: Creating University Users with Different Privileges

Create Users

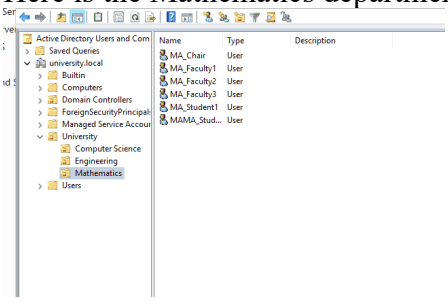
6 users were created for each appartment, the Chair, 2 Faculty, and 3 Students
Here is the Computer Science department



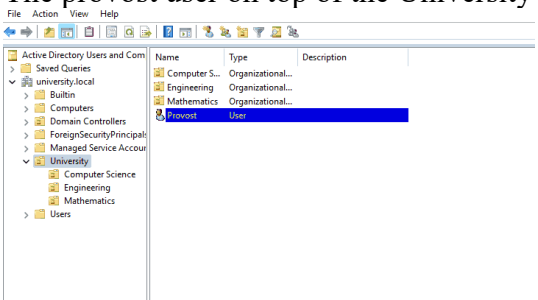
Here is the Engineering department



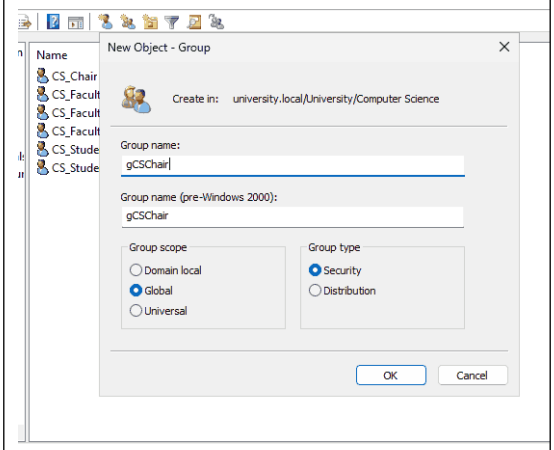
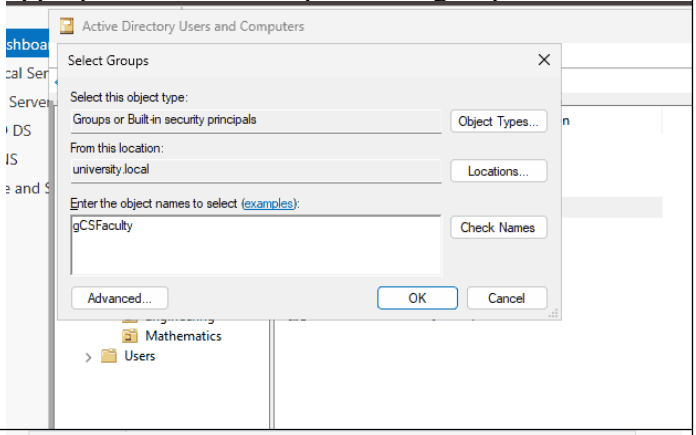
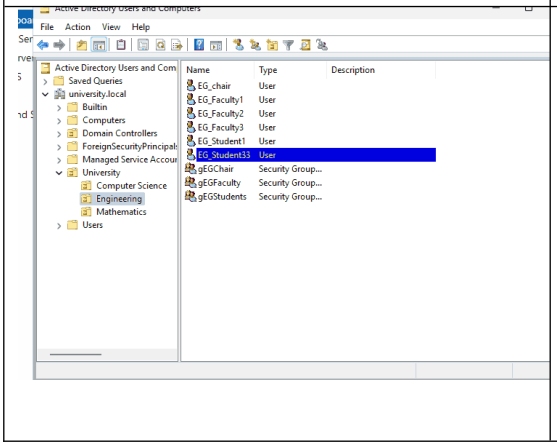
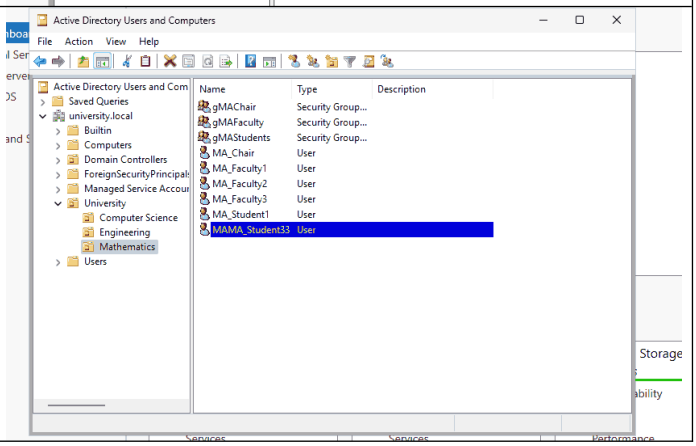
Here is the Mathematics department



The provost user on top of the University



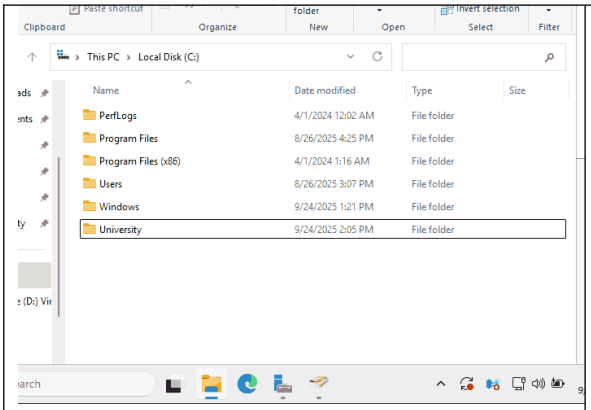
Create Security Groups

This is the pop-up for creating a new group	9 groups were created, gCSChair, gCSFaculty, gEGStudent, gEGChair, gEGFaculty, gEGStudent, gMAChair, gMAFaculty, gMAStudent, and the appropriate users were put in the group.
	
	

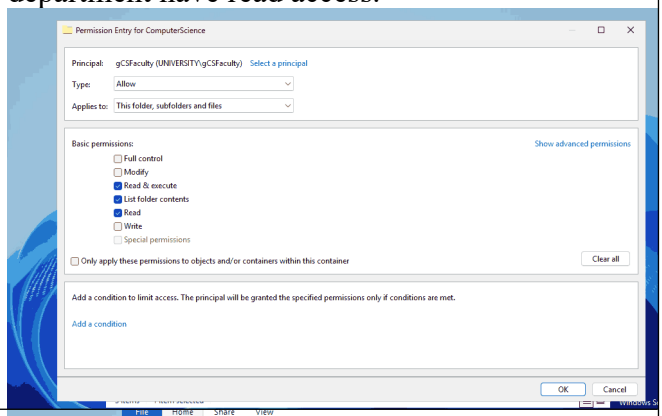
Task 4: Task 4: Setting Up Folder Permissions

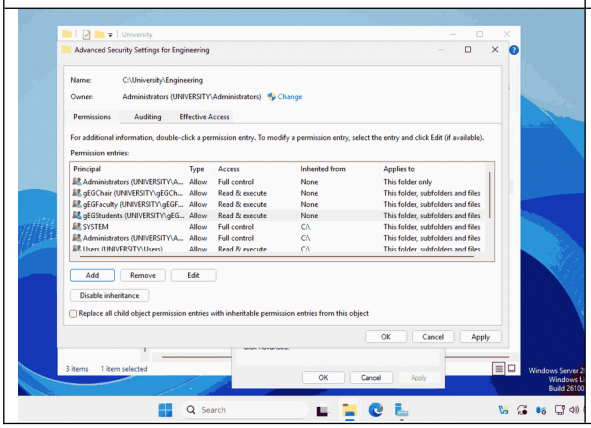
Create Departmental Folders and assign permissions

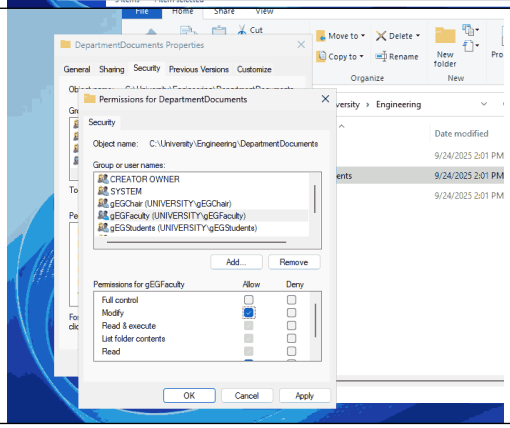
Created the University document and the subfolders for each department, which are announcements, departmentDocuments, and SharedResources	Used the powershell scripts to assign all the positions. The provost users as the owner and The chair has write access for their department folder, the Faculy write access for DepartmentDocuments and SharedResources and Students have write access for just the SharedResources. Lastly All users inside the



department have read access.



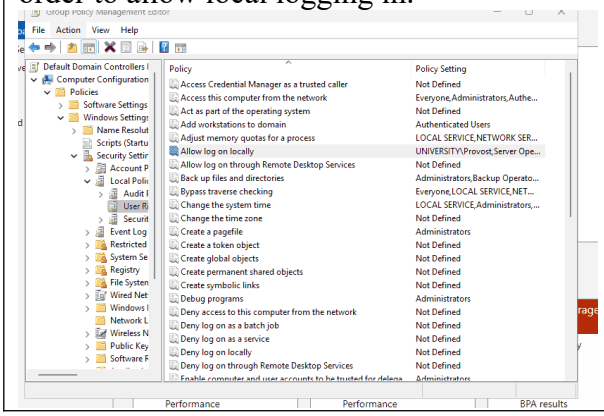




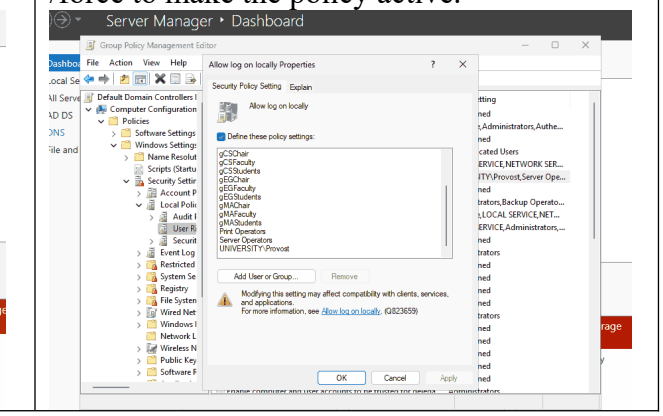
Task 5: Verifying all settings

Enable local logon of domain users onto the domain controller

Opened Group Policy Management Editor, in order to allow local logging in.

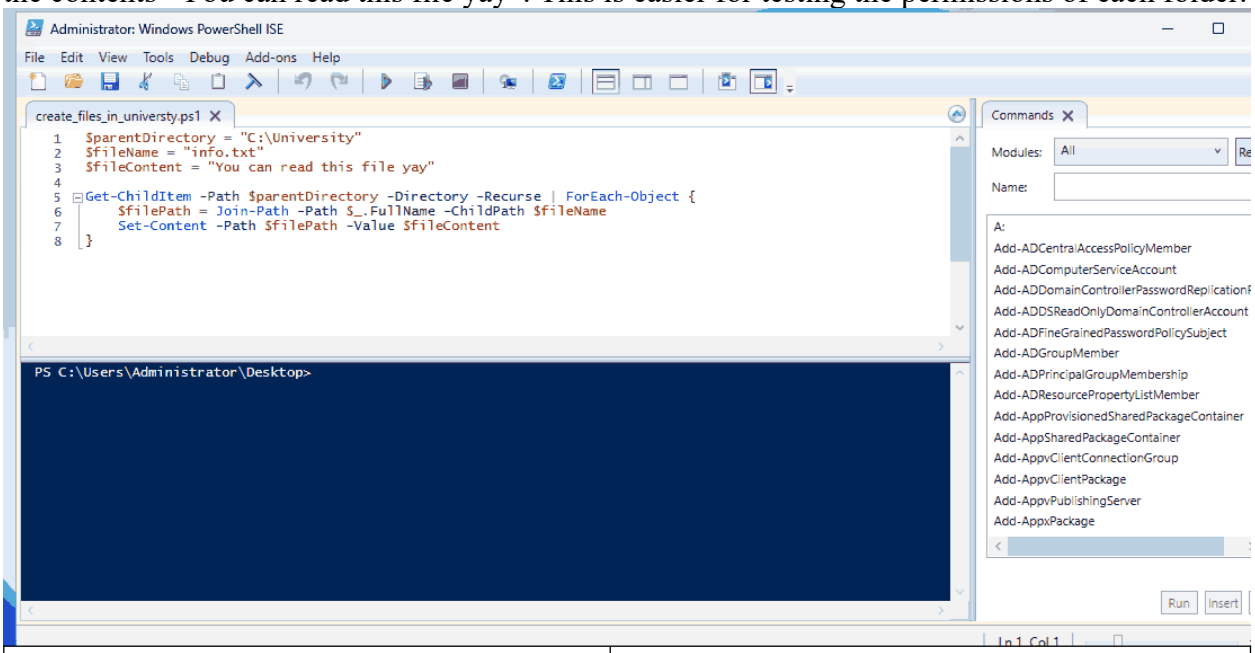


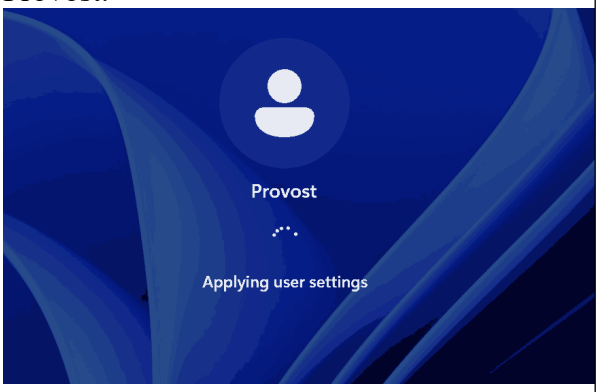
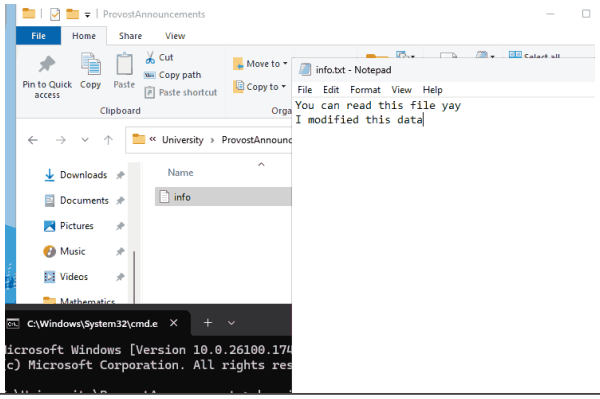
Added all the groups in and did a gpupdate /force to make the policy active.

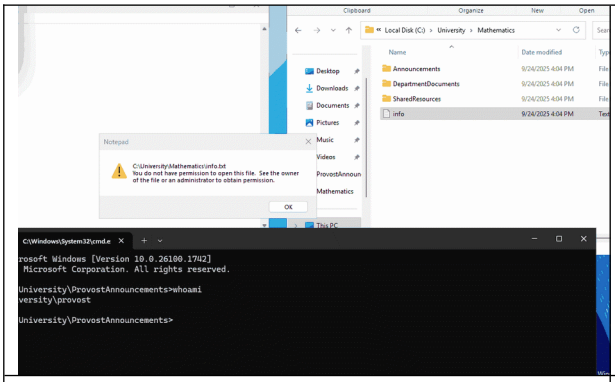


Verifying all settings

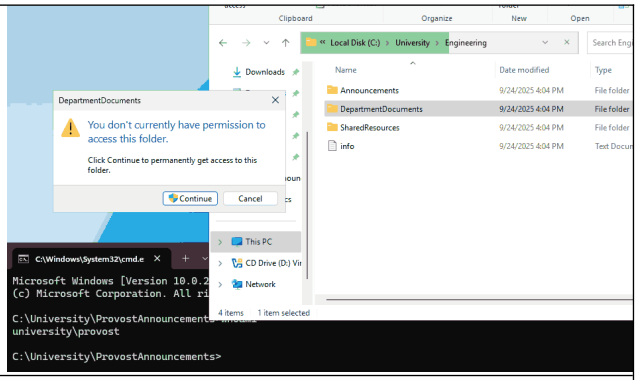
I created a script that creates a file for each directory in the University folder, all of them have the contents “You can read this file yay”. This is easier for testing the permissions of each folder.



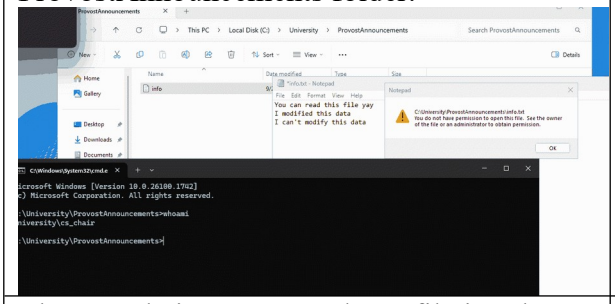
Signed out of Administrator and logged in to Provost.	I was able to modify the file inside the ProvostAnouncements.
	
The provost user does not have read permissions for any of the departments.	The provost user does not have file listing for any of the subfolders in the departments.



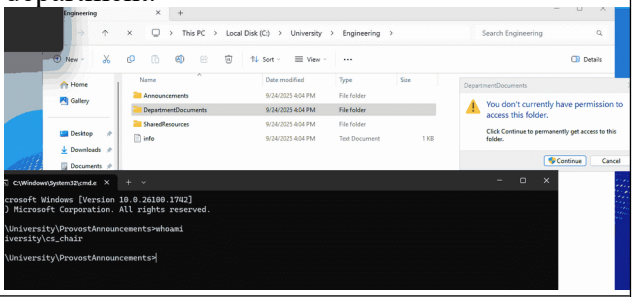
The CS chair cannot modify the ProvostAnnouncements folder.



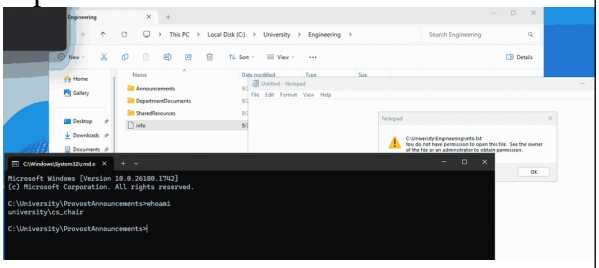
The CS chair does not have access in any other department.



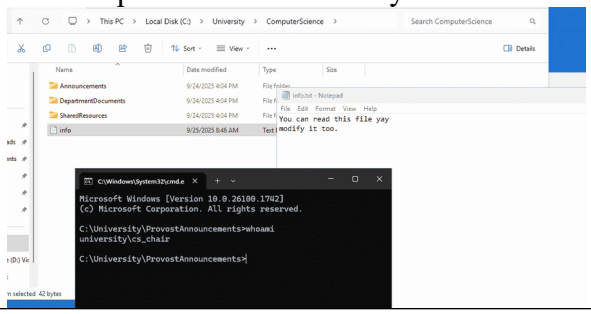
The CS Chair cannot read any file in other departments.



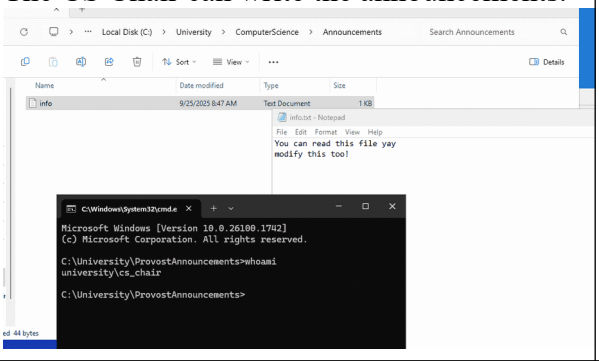
The CS chair can read and write everything it the ComputerScience directory.



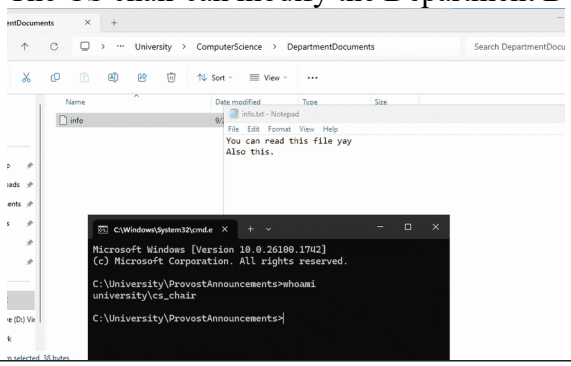
The CS Chair can write the announcements.



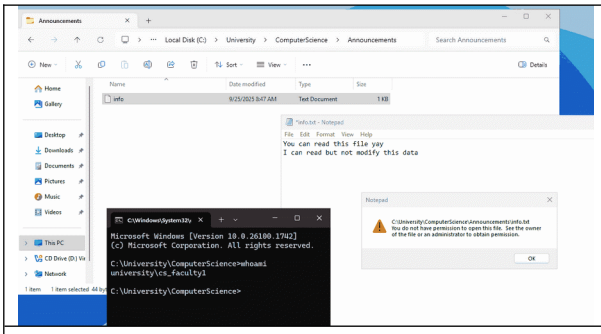
The CS chair can modify the Department Docs.



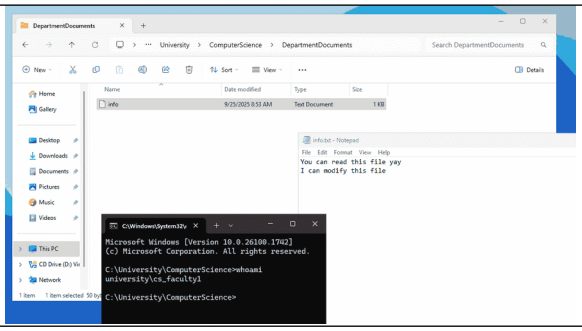
CS faculty cannot modify the anouncements.



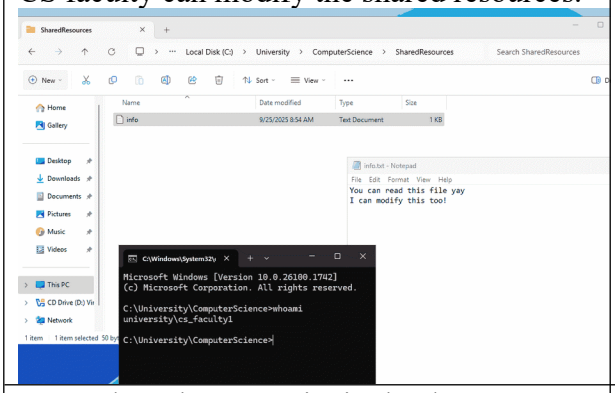
CS faculty can modify the department docs.



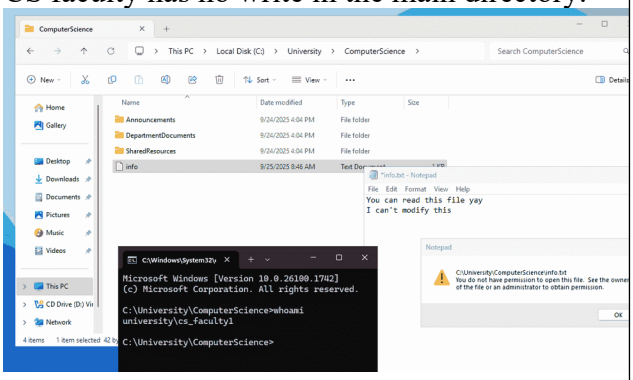
CS faculty can modify the shared resources.



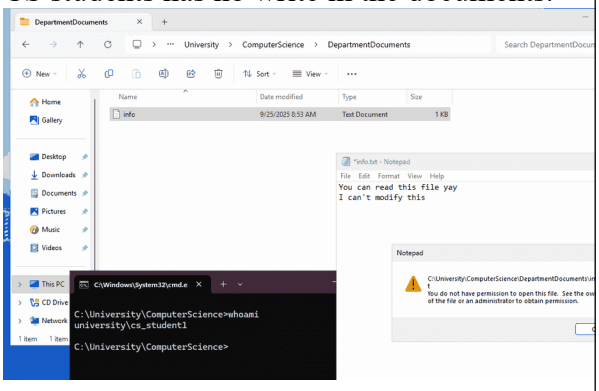
CS faculty has no write in the main directory.



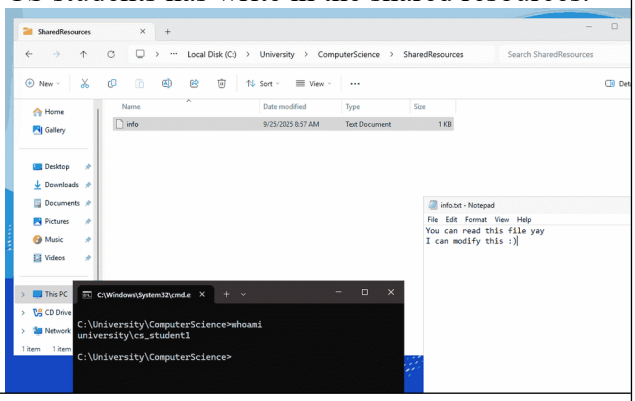
CS students has no write in the documents.



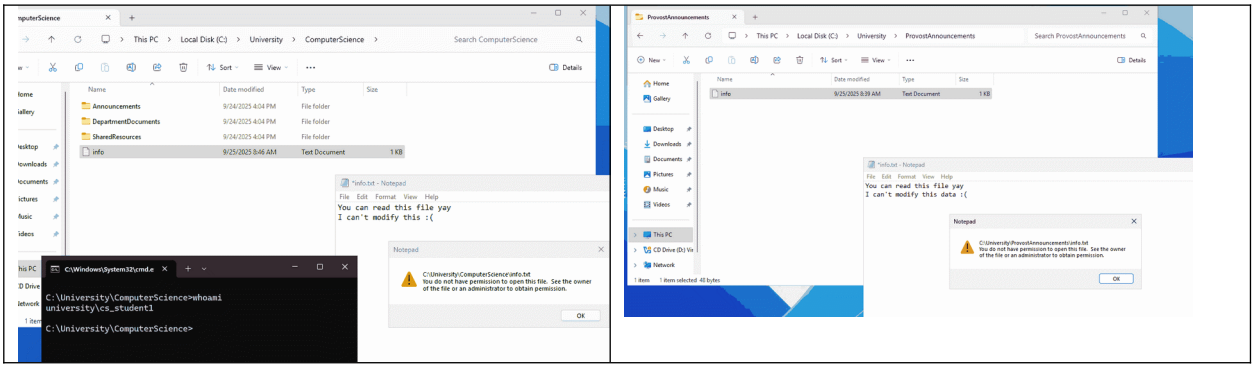
CS students has write in the shared resources.



CS students has no write in main directory.



CS students no write in the announcements.



Conclusions

The lab taught me a lot on how active directory works on windows. I learned how to create Ous and domains, how to create groups and users, configuring their permissions, so that they have either read, write or full permissions for each folder. I have learned how secure passwords policies work and enable them. I have learned about the group policy editor and how they can contain settings for the organization such as local login and password policies. I have delved into PowerShell scripting and how they can automate the process of creating users/groups and setting their permissions. Lastly, I have learned how to verify the permissions of each folder knowing who has access and what they can do with them. The output of the lab is a working windows server domain with the users and groups with the retrospective folders for them.

References

https://github.com/ufidon/comsec/blob/main/labs/lab03/README.md