Name: Cabal, Krizanto Kyle B.
Course & Section: BSIT 4-3

LAB 2 Laboratory: User Management and Permissions in Windows

Objective:

Students will learn how to manage user accounts and groups, and assign permissions to files and folders in Windows using both graphical and command-line interfaces. By the end of this activity, students will be able to create, modify, and delete users and groups, as well as assign permissions to different user groups.

Lab Setup:

1. **Operating System:** Windows 10 or later.
2. **Required Tools:**
   - Command Prompt with Administrator privileges.
   - Access to the Local Users and Groups tool (lusrmgr.msc).
   - A folder created on the system for testing permissions (e.g., C:\LabFiles).

Task 1: Creating Users via Command Prompt

Step 1: Open Command Prompt as Administrator.

   - Search for **cmd** in the Start menu, right-click, and select **Run as administrator**.
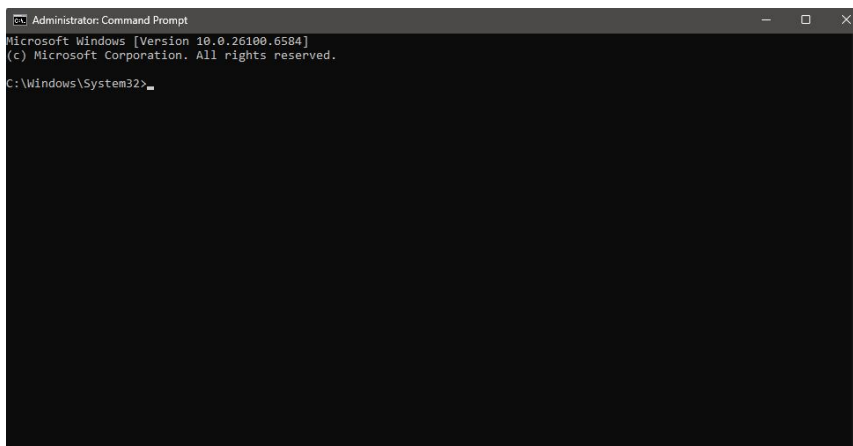
Step 2: Create two users (student1 and student2):
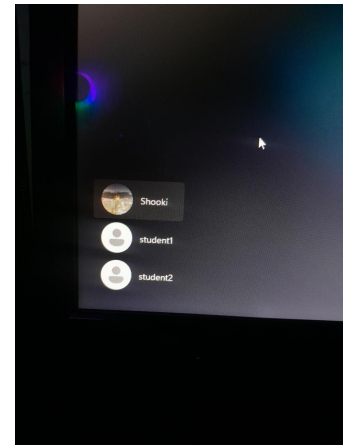net user student1 password123 /add
net user student2 password456 /add

Step 3: Verify the users were created:

net user student1

net user student2

Task 2: Creating User Groups and Adding Users to Groups

Step 1: Create a group called "LabGroup":

net localgroup LabGroup /add

Step 2: Add both users (student1 and student2) to "LabGroup":

net localgroup LabGroup student1 /add

net localgroup LabGroup student2 /add

```
C:\Windows\System32>net localgroup LabGroup student1 /add
The command completed successfully.


C:\Windows\System32>net localgroup LabGroup student2 /add
The command completed successfully.
```

Step 3: Verify that the users were added to the group:
net localgroup LabGroup

```
C:\Windows\System32>net localgroup LabGroup
Alias name      LabGroup
Comment

Members

-------------------------------------------------------------
student1
student2
The command completed successfully.
```

Task 3: Setting Folder Permissions for the Group

Step 1: Create a folder called "C:\LabFiles":

- ○ Use File Explorer or:
  mkdir C:\LabFiles

```
C:\Windows\System32>mkdir C:\LabFiles
```

Step 2: Assign full control of the "C:\LabFiles" folder to the group "LabGroup":
icacls "C:\LabFiles" /grant LabGroup:F

```
C:\Windows\System32>icacls "C:\LabFiles" /grant LabGroup:F
processed file: C:\LabFiles
Successfully processed 1 files; Failed processing 0 files
```

Step 3: Verify that the group has the correct permissions on the folder:
icacls "C:\LabFiles"

```
C:\Windows\System32>icacls "C:\LabFiles"
C:\LabFiles DESKTOP-J8UGSAV\LabGroup:(F)
            BUILTIN\Administrators:(I)(OI)(CI)(F)
            NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)
            BUILTIN\Users:(I)(OI)(CI)(RX)
            NT AUTHORITY\Authenticated Users:(I)(M)
            NT AUTHORITY\Authenticated Users:(I)(OI)(CI)(IO)(M)

Successfully processed 1 files; Failed processing 0 files
```

Task 4: Modifying and Testing User Permissions

Step 1: Remove write permissions for student2 on the "C:\LabFiles" folder:
icacls "C:\LabFiles" /deny student2:W

```
C:\Windows\System32>icacls "C:\LabFiles" /deny student2:W
processed file: C:\LabFiles
Successfully processed 1 files; Failed processing 0 files
```

Step 2: Test the permissions:

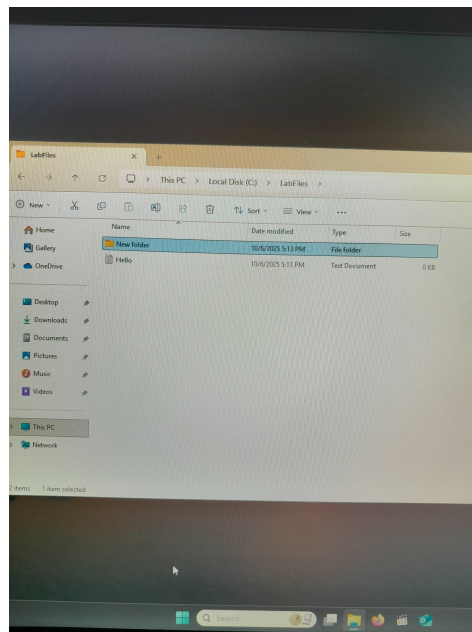- **Log in as student2** and try to create a file in the "C:\LabFiles" folder. They should be denied access.
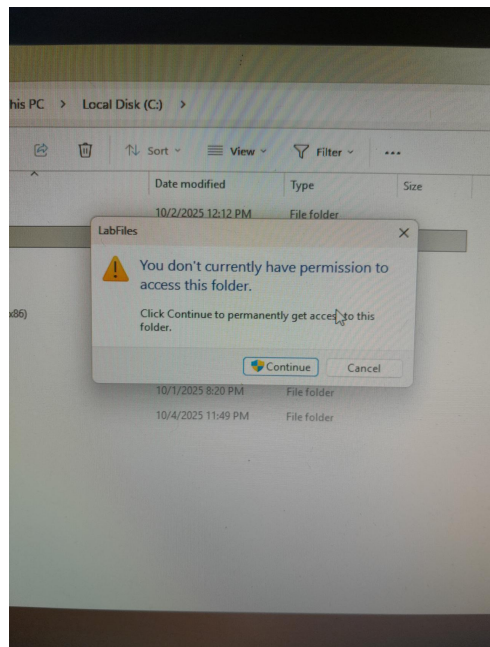
- **Log in as student1** and create a file in the "C:\LabFiles" folder, which should succeed.

Task 5: Deleting Users and Groups

Step 1: Remove the users from the group

net localgroup LabGroup student1 /delete

net localgroup LabGroup student2 /delete

```
C:\Windows\System32>net localgroup LabGroup student1 /delete
The command completed successfully.


C:\Windows\System32>net localgroup LabGroup student2 /delete
The command completed successfully.
```

Step 2: Delete the users:

net user student1 /delete

net user student2 /delete

```
C:\Windows\System32>net user student1 /delete
The command completed successfully.


C:\Windows\System32>net user student2 /delete
The command completed successfully.
```

Step 3: Delete the group:

net localgroup LabGroup /delete

```
C:\Windows\System32>net localgroup LabGroup /delete
The command completed successfully.
```

1. Why do you think it's important to have different types of user accounts (e.g., admin vs. regular user)?

　　　- It's important to have different user accounts because admins need more control to manage the system, while regular users should only access basic features. This helps keep the system organized and secure.

2. What would happen if someone accidentally had admin access?

　　　- If someone accidentally had admin access, they could change or delete important data, settings, or accounts. This could cause system problems or security risks.

3. If everyone had full access to all files, what issues might arise in a company setting?

　　　- If everyone had full access, people could accidentally delete or change important files, cause data leaks, or expose private information. This could lead to confusion and security problems.

4. Why is it important to know how to change permissions on different operating systems?

　　　- It's important to know how to change permissions so you can protect files, control who can access them, and keep the system safe from mistakes or unauthorized changes.

5. Why do you think grouping users would make the job of an administrator easier?

　　　- Grouping users makes an administrator's job easier because they can set permissions or rules for many users at once instead of doing it one by one.

6. What could happen if we did not regularly audit users and permissions in an organization?

　　　- If we don't regularly check users and permissions, old or unused accounts might stay active, leading to security leaks, data leaks, or unauthorized access.

7. What steps would you take to create this user and assign the correct permissions?

　　　- To create a user and assign the correct permissions, I would open Command Prompt as Administrator and use the command net user <username> <password> /add to create a new user. Then, I would create a group using net localgroup <groupname> /add and add the user to that group with net localgroup <groupname> <username> /add. After that, I'd set folder permissions using icacls <folderpath> /grant <groupname>:F, and adjust access if needed with commands like icacls <folderpath> /deny <username>:W.