Lab: Windows 11 User Accounts Management

Objective:

By the end of this lab, students will be able to manage user accounts in Windows 11, configure access controls, set up password policies, understand authentication methods, and apply group policies.

Materials Needed:

- A computer running Windows 11.
- Administrator access to the Windows 11 machine.

Steps:

Part 1: Managing User Accounts

1. **Create a New User Account:**
   - Open the **Settings** app by pressing `Windows + I`.
   - Navigate to **Accounts** > **Family / other users**.
   - Click on **Add account** under "Other users."
   - Choose **"I don't have this person's sign-in information"** and then **"Add a user without a Microsoft account"**.
   - Enter a username and password for the new local account.
   - Assign the account type as **Administrator** or **Standard user** depending on the requirement.
2. **Switch User Accounts:**
   - Sign out of your current account by clicking on the **Start menu** > **Your Profile Icon** > **Sign out**.
   - Sign in with the newly created account.
3. **Delete a User Account:**
   - Go back to **Settings** > **Accounts** > **Family & other users**.
   - Select the user account you wish to delete and click **Remove**.
   - Choose whether to delete the user's files or keep them.

Part 2: Configuring Access Controls

1. **Set Up Access Control for a User:**
   - Right-click on the **Start menu** and select **Computer Management**.
   - Go to **Local Users and Groups** > **Users**.
   - Right-click on the user account and select **Properties**.
   - Under the **General** tab, configure account settings such as account disabling, password requirements,
   - Use the **Member Of** tab to add or remove the user from groups, which determines their access level to system resources.
2. **Manage File and Folder Permissions:**
   - Right-click on any file or folder and select **Properties**.
   - Go to the **Security** tab.

- Click **Edit** to change permissions for different users or groups.
- Set the desired permissions (Full control, Modify, Read & execute, etc.) and click **Apply**.

Part 3: Setting Up Password Policies

1. **Configure Local Password Policies:**
    - Press `Windows + R`, type `secpol.msc`, and press Enter to open the Local Security Policy.
    - Navigate to **Account Policies** > **Password Policy**.
    - Configure the following settings:
        - **Enforce password history:** Set the number of unique new passwords that must be used before an old password can be reused.
        - **Maximum password age:** Set the number of days a password can be used before the system requires a change.
        - **Minimum password age:** Set the number of days that a password must be used before it can be changed.
        - **Minimum password length:** Set the minimum number of characters required for a password.
        - **Password must meet complexity requirements:** Enable to require complex passwords.
        - **Store passwords using reversible encryption:** Should generally be disabled for security reasons.
2. **Test the Password Policy:**
    - Attempt to change the password of an account to ensure the policies are enforced.
    - Try to set a password that doesn’t meet the complexity or length requirements to see how the system responds.

Part 4: Exploring Authentication Methods

1. **Set Up Windows Hello:**
    - Go to **Settings** > **Accounts** > **Sign-in options**.
    - Under **Windows Hello**, set up facial recognition, fingerprint, or PIN.
    - Follow the prompts to complete the setup.
2. **Configure Two-Factor Authentication:**
    - If using a Microsoft account, go to the Microsoft account website and enable two-factor authentication under the **Security** settings.
    - Choose your preferred second factor, such as a phone number or an authentication app.
3. **Manage Authentication Methods:**
    - In **Sign-in options**, review and manage other available authentication methods such as security keys or dynamic lock.

Part 5: Applying Group Policies

1. **Access the Group Policy Editor:**
    - Press `Windows + R`, type `gpedit.msc`, and press Enter to open the Group Policy Editor.
2. **Configure Group Policies:**

    - Navigate through **Computer Configuration** or **User Configuration** to find specific policies to apply.
    - For example, under **Computer Configuration** > **Administrative Templates** > **System** > **Logon**, you can enforce certain logon settings like "Do not display last user name."

3. **Enforce a Policy:**
    - Double-click on a policy setting, enable or disable it, and click **Apply**.
    - Common policies to apply include restricting access to control panel items, enforcing password policies, or managing user profiles.
4. **Apply Group Policy to a Specific User:**
    - Use the **Group Policy Management Console** (GPMC) if you're in a domain environment, or edit the **Local Group Policy** directly.
    - Create or link Group Policy Objects (GPOs) to organizational units (OUs) to apply policies to specific users or groups.

Part 6: Testing and Reporting

1. **Test the Applied Policies and Settings:**
    - Log in as a standard user and check if the configured policies and access controls are enforced.
    - Verify that password policies are working by attempting to change the password.
2. **Create a Lab Report:**
    - Include screenshots of the user accounts created, password policies configured, and group policies applied.
    - Reflect on the importance of managing user accounts, access controls, and policies in a Windows environment.
    - Discuss any issues encountered and how they were resolved.