Hardware/Operating System Technology (ITI-2640-01)

Completed By: Luswepo Daniel Sinyinza
Project Title: Enhancing Password Security for Lobby Windows Laptop

Project Overview:
As a student taking on the role of an IT administrator responsible for a small corporate network, the objective of this project is to enhance the password security for the windows laptop located in the Lobby. This endeavor will involve the configuration of password policies and account lockout policies using the Local Security Policy tool, ensuring the laptop remains secure and user accounts are well-protected.

Project Objectives:

Implement Password Policies:

1. Ensure that new passwords cannot be the same as the previous four passwords.
2. Require users to change their passwords every 30 days.
3. Prevent users from changing their new passwords for at least two days.
4. Set a minimum password length of 10 characters.
5. Enforce the inclusion of non-alphabetical characters in passwords.

Implement Account Lockout Policies:

6. Lock user accounts after four incorrect login attempts.
   - Automatically unlock locked accounts after 60 minutes.
   - Reset the failed login counter to 0 after 40 minutes.

Project Steps:

Step 1: Accessing the Local Security Policy Tool

- Log in to the windows laptop located in the Lobby as an administrator.
- Navigate to the "Local Security Policy" tool using the following steps:
- Press Win + R to open the Run dialog.
- Type **secpol.msc** and press Enter to open the Local Security Policy window.

Step 2: Configure Password Policies
Policy 1: Enforce Password History

- In the Local Security Policy window, navigate to "Account Policies" > "Password Policy."
- Double-click on "Enforce password history" in the right pane.
- Set the value to "4 passwords remembered."

Policy 2: Maximum Password Age

- Still in the "Password Policy" section, double-click on "Maximum password age."
- Set the value to "30 days."

Policy 3: Minimum Password Age

- Double-click on "Minimum password age."
- Set the value to "2 days."

Policy 4: Minimum Password Length

- Double-click on "Minimum password length."
- Set the value to "10 characters."

Policy 5: Password Must Meet Complexity Requirements

- Double-click on "Password must meet complexity requirements."
- Ensure this policy is set to "Enabled."

Step 3: Configure Account Lockout Policies

Policy 6: Account Lockout Threshold

- In the Local Security Policy window, navigate to "Account Policies" > "Account Lockout Policy."
- Double-click on "Account lockout threshold."
- Set the value to "4 invalid logon attempts."

Policy 7: Account Lockout Duration

- Double-click on "Account lockout duration."
- Set the value to "60 minutes."

Policy 8: Reset Account Lockout Counter After

- Double-click on "Reset account lockout counter after."
- Set the value to "40 minutes."

Step 4: Testing and Monitoring

- After configuring these policies, it's essential to thoroughly test their implementation to ensure they function as expected.
- Monitor user accounts to verify that password changes and account lockouts occur according to the configured policies.
- Continuously review and adjust these policies as necessary to maintain a high level of password security.

Project Completion:
Upon the successful configuration of the specified password and account lockout policies, the Windows laptop in the Lobby will have significantly improved password security. Users will be required to create strong, non-repetitive passwords, and the account lockout policies will help protect against unauthorized access attempts.