Windows 11 Local Security Policy Lab

Lab Objectives

- Access and navigate Local Security Policy.

- Configure password policies.

- Set account lockout policies.

- Configure audit policies.

- Assign user rights.

- Configure security options.

Lab Prerequisites

- A Windows 11 machine with administrator access.
- Basic familiarity with Windows 11 settings.

Exercise 1: Accessing Local Security Policy

1. Open Local Security Policy:
   - Press Win + R, type secpol.msc, and press Enter.
   - The Local Security Policy window should open.

2. Explore the Local Security Policy categories:
   - Click through each of the sections on the left panel to familiarize yourself with categories such as Account Policies, Local Policies, Event Log, and Public Key Policies.

- Questions:
  - - What sections are available in the Local Security Policy window?
  - - Why is it important to control local security policies on a Windows system?

Exercise 2: Configure Password Policies

1. In the Local Security Policy window, go to Account Policies > Password Policy.
2. Configure the following settings:
   - Minimum password length: Set it to 8 characters.
   - Password must meet complexity requirements: Enable this option.
   - Enforce password history: Set it to remember the last 5 passwords.

3. Apply and save the changes.

- Questions:

- - What does enabling password complexity require users to include in their passwords?
- - Why is setting a minimum password length beneficial?

Exercise 3: Set Account Lockout Policies

1. Navigate to Account Policies > Account Lockout Policy.
2. Configure the following settings:
   - Account lockout threshold: Set to 3 invalid login attempts.
   - Account lockout duration: Set to 30 minutes.
   - Reset account lockout counter after: Set to 30 minutes.

3. Save and close the settings.

- Questions:
  - - What is the purpose of an account lockout policy?
  - - How might a strict account lockout policy affect user experience and security?

Exercise 4: Configure Audit Policies

1. In the Local Policies section, click on Audit Policy.
2. Enable auditing for the following:
   - Audit logon events: Set to Success, Failure.
   - Audit account management: Set to Success, Failure.
   - Audit policy change: Set to Success, Failure.

3. Apply the settings and close the window.

- Questions:
  - - Why would you want to audit logon events and account management?
  - - Where can you view the audit logs after they are generated?

Exercise 5: Assign User Rights

1. In the Local Policies section, go to User Rights Assignment.
2. Find and configure the following rights:
   - Deny log on locally: Add a test user account to this policy to prevent them from logging in.
   - Allow log on through Remote Desktop Services: Add a specific user or group who should be allowed remote access.

3. Save and apply the changes.

- Questions:
  - - Why is it useful to control logon rights for specific users or groups?
  - - What could be the security implications of allowing too many users remote access?

Exercise 6: Configure Security Options

1. Go to Local Policies > Security Options.
2. Find and configure the following:
   - Accounts: Limit local account use of blank passwords to console logon only: Set this to Enabled.
   - Interactive logon: Do not display last user name: Set this to Enabled.
   - Network security: LAN Manager authentication level: Set to Send NTLMv2 response only. Refuse LM & NTLM.

3. Apply and save the settings.

- Questions:
  - - Why is it advisable to disable displaying the last logged-in username?
  - - What benefits does limiting the use of blank passwords provide?

Exercise 7: Review and Test the Policy Changes

1. Restart your computer for the changes to take effect fully.
2. Test each configured policy by attempting the following:
   - Log in with an incorrect password multiple times to test the account lockout.
   - Attempt to log in with the test user account assigned to “Deny log on locally” to confirm it’s working.
   - Check the Event Viewer under Security logs to view the auditing logs for logon events and policy changes.

- Questions:
  - - Were the configurations effective based on your tests?
  - - How can you use these settings to balance security with usability?

Conclusion

You have now configured and tested key elements of the Windows 11 Local Security Policy. Understanding these policies can help improve security on individual devices or across a network.