Password Policies for Local Windows Accounts - Practical Activities

Dr. Brahim Ferik

Practical Activities

This section provides a set of practical activities designed to help students apply the concepts learned in managing local Windows accounts and password policies.

Activity 1: Create a New User and Apply Password Policies

Objective:

To create a new user account and apply password policies to ensure security.

Steps:

1. Create a new user without a password:

   ```
   net user username /add
   ```

2. Set a strong password for the user:

   ```
   net user username StrongP@ssw0rd!
   ```

3. Open the Local Security Policy to configure password policies:

   ```
   Win + R : secpol.msc
   ```

4. Configure the following password policies:
   - Enforce password history: 5 passwords.
   - Maximum password age: 90 days.
   - Minimum password length: 8 characters.
   - Password must meet complexity requirements: Enabled.

Activity 2: Test Account Lockout Policy

Objective:

To test the account lockout policy by simulating failed login attempts.

Steps:

1. Open the Local Security Policy:

   ```
   Win + R : secpol.msc
   ```

2. Navigate to **Account Policies > Account Lockout Policy**.

3. Configure the following settings:
    - Account lockout threshold: 3 invalid logon attempts.
    - Account lockout duration: 15 minutes.
    - Reset account lockout counter after: 5 minutes.
4. Attempt to log in with an incorrect password multiple times to trigger the lockout.
5. Verify that the account is locked out by attempting to log in again.
6. Wait for the lockout duration to expire or unlock the account manually using:

```
net user username /active:yes
```

Activity 3: Review Events in Event Viewer

Objective:

To monitor successful and failed login attempts using Event Viewer.

Steps:

1. Enable audit logon events in the Local Security Policy:

```
Win + R : secpol.msc
```

2. Navigate to **Advanced Audit Policy Configuration > Logon/Logoff**.
3. Enable **Audit Logon** for both success and failure.
4. Attempt to log in successfully and unsuccessfully to generate events.
5. Open Event Viewer:

```
Win + R : eventvwr.msc
```

6. Navigate to **Windows Logs > Security**.
7. Review the following events:
    - Event ID 4624: Successful logon.
    - Event ID 4625: Failed logon.

Activity 4: Design Comprehensive Security Policies

Objective:

To design comprehensive security policies for a hypothetical organization.

Steps:

1. Divide students into groups.
2. Instruct each group to design security policies covering:
    - Password policies (e.g., length, complexity, expiration).
    - Account lockout policies (e.g., thresholds, durations).
    - Logon/logoff policies (e.g., auditing, monitoring).
3. Present the proposed policies in a group presentation.
4. Discuss the effectiveness of each policy and its implementation.