Laboratory Exercise: Implementing Password Security Policies on Windows 10

Learning Objectives

- Implement IT security policies focusing on access control
- Configure password complexity and expiration requirements using Group Policy
- Apply security best practices to safeguard organizational assets
- Understand the role of compliance in password management

Lab Overview

Duration: 90-120 minutes
Environment: Windows 10 Virtual Machine (Pro or Enterprise edition)
Prerequisites: Administrator access, basic understanding of Windows administration

---

Scenario

You are an IT administrator for a small company. Management has tasked you with implementing a new password security policy to comply with industry standards and protect against unauthorized access. You must configure the system to enforce strong passwords and regular password changes.

Company Password Security Policy Document

Your company has approved the following password policy:

Password Complexity Requirements:

- Minimum password length: **[MIN_LENGTH]** characters
- Password must meet complexity requirements (uppercase, lowercase, numbers, symbols)
- Password history: Remember last **[HISTORY_COUNT]** passwords
- Minimum password age: **[MIN_AGE]** day(s)
- Maximum password age: **[MAX_AGE]** days
- Account lockout threshold: **[LOCKOUT_THRESHOLD]** invalid attempts
- Account lockout duration: **[LOCKOUT_DURATION]** minutes
- Reset account lockout counter after: **[RESET_COUNTER]** minutes

Required Values (Instructor will provide):

- **[MIN_LENGTH]** = ______
- **[HISTORY_COUNT]** = ______
- **[MIN_AGE]** = ______
- **[MAX_AGE]** = ______
- **[LOCKOUT_THRESHOLD]** = ______
- **[LOCKOUT_DURATION]** = ______
- **[RESET_COUNTER]** = ______

Part 1: Understanding Current Security Settings (15 minutes)

Task 1.1: Access Local Security Policy

1. Press `Win + R` to open Run dialog
2. Type: `secpol.msc` and press Enter
3. Navigate through the following sections and document current settings:

Account Policies → Password Policy:

- Take a screenshot showing all current password policy settings
- Document each setting's current value

Account Policies → Account Lockout Policy:

- Take a screenshot showing all current lockout settings
- Document each setting's current value

Task 1.2: Check Current User Password Information

Open Command Prompt as Administrator and run:

```
net user [USERNAME]
```

Replace `[USERNAME]` with your test username.

Deliverable:

- Screenshots of current Local Security Policy settings
- Screenshot of `net user` output
- Document all current values in a table

Part 2: Creating Test Users (10 minutes)

Task 2.1: Create Test Users via Command Prompt

Open Command Prompt as Administrator:

```
net user testuser1 TempPass123! /add
net user testuser2 TempPass123! /add
net user testuser3 TempPass123! /add
```

Task 2.2: Verify User Creation

```
net user
net user testuser1
```

Deliverable: Screenshot showing the three test users created.

Part 3: Configuring Password Policy (30 minutes)

Task 3.1: Access Password Policy Settings

1. Open Local Security Policy (`secpol.msc`)
2. Navigate to: **Security Settings** → **Account Policies** → **Password Policy**

Task 3.2: Configure Password Complexity Settings

Configure each policy according to the company requirements:

1. Enforce password history

- Double-click the policy
- Set to: **[HISTORY_COUNT]** passwords remembered
- Click Apply, then OK

2. Maximum password age

- Double-click the policy
- Set to: **[MAX_AGE]** days
- Click Apply, then OK

3. Minimum password age

- Double-click the policy
- Set to: **[MIN_AGE]** day(s)
- Click Apply, then OK

4. Minimum password length

- Double-click the policy
- Set to: **[MIN_LENGTH]** characters
- Click Apply, then OK

5. Password must meet complexity requirements

- Double-click the policy
- Set to: **Enabled**
- Click Apply, then OK

Note: When enabled, passwords must contain characters from three of the following four categories:

- *Uppercase letters (A-Z)*
- *Lowercase letters (a-z)*
- *Numbers (0-9)*
- *Special characters (!@#$%^& etc.)**

6. Store passwords using reversible encryption

- Double-click the policy
- Ensure this is set to: **Disabled**
- Click Apply, then OK

Task 3.3: Apply the New Policy

Open Command Prompt as Administrator:

```
gpupdate /force
```

Deliverable:

- Screenshot showing all configured password policies
- Screenshot of successful `gpupdate` execution

Part 4: Testing Password Complexity Requirements (25 minutes)

Task 4.1: Test Password Policies

For **testuser1**, attempt to change the password using various combinations. Document which passwords are accepted or rejected and explain why.

Open Command Prompt as Administrator:

```
net user testuser1 [NEW_PASSWORD]
```

Test these passwords and document the results:

Password Attempt	Expected Result	Actual Result	Reason
`Pass123`			
`password`			
`PASSWORD123`			
`P@ssw0rd`			
`MySecureP@ss123`			
`testuser1`			

Task 4.2: Verify Password Age Settings

After successfully setting a compliant password for testuser1:

```
net user testuser1
```

Look for:

- Password last set
- Password expires
- Password changeable

Deliverable:

- Completed test results table with explanations
- Screenshot showing password age information
- Brief explanation of why complexity requirements improve security

Part 5: Configuring Account Lockout Policy (25 minutes)

Task 5.1: Access Account Lockout Policy Settings

1. In Local Security Policy (`secpol.msc`)
2. Navigate to: **Security Settings** → **Account Policies** → **Account Lockout Policy**

Task 5.2: Configure Lockout Settings

Configure the following policies according to company requirements:

1. Account lockout duration

- Double-click the policy
- Set to: **[LOCKOUT_DURATION]** minutes
- Click Apply, then OK

2. Account lockout threshold

- Double-click the policy
- Set to: **[LOCKOUT_THRESHOLD]** invalid logon attempts
- Click Apply, then OK

Note: Windows will automatically suggest a value for "Reset account lockout counter after"

3. Reset account lockout counter after

- Verify it's set to: **[RESET_COUNTER]** minutes
- Adjust if necessary
- Click Apply, then OK

Task 5.3: Apply the Lockout Policy

```
gpupdate /force
```

Deliverable:

- Screenshot showing all three configured lockout policies
- Explanation of how these three settings work together

Part 6: Testing Account Lockout Policy (20 minutes)

Task 6.1: Simulate Failed Login Attempts

Method 1: Using Command Prompt

Attempt to log in as testuser2 with incorrect password:

```
runas /user:testuser2 cmd
```

Enter an incorrect password **[LOCKOUT_THRESHOLD]** times.

Method 2: Using Windows Login Screen

1. Lock your workstation (Win + L)
2. Click "Other user"
3. Enter username: `testuser2`
4. Enter incorrect password **[LOCKOUT_THRESHOLD]** times
5. Observe the lockout message

Task 6.2: Verify Account Lockout

Open Command Prompt as Administrator:

```
net user testuser2
```

Look for: **Account active: Locked**

Task 6.3: View Lockout Events (Optional)

1. Open Event Viewer (`eventvwr.msc`)
2. Navigate to: **Windows Logs** → **Security**
3. Filter for Event ID: **4740** (Account lockout)

Task 6.4: Unlock the Account

Option 1: Wait for automatic unlock

- Wait **[LOCKOUT_DURATION]** minutes

Option 2: Manually unlock

```
net user testuser2 /active:yes
```

Deliverable:

- Screenshot showing locked account status
- Screenshot of Event Viewer showing lockout event (Event ID 4740)
- Screenshot showing account after unlock
- Explanation of when manual vs automatic unlock should be used

Part 7: Testing Password History (15 minutes)

Task 7.1: Change Password Multiple Times

For testuser3, change the password several times:

```
net user testuser3 [NEW_PASSWORD_1]
net user testuser3 [NEW_PASSWORD_2]
net user testuser3 [NEW_PASSWORD_3]
```

Task 7.2: Attempt to Reuse Old Password

Try to change the password back to **[NEW_PASSWORD_1]**:

```
net user testuser3 [NEW_PASSWORD_1]
```

Deliverable:

- Screenshot showing the error when attempting to reuse a password
- Explanation of why password history prevents security risks
- Document how many times you need to change the password before you can reuse **[NEW_PASSWORD_1]**

Part 8: Creating a Security Compliance Report (20 minutes)

Task 8.1: Export Current Security Policy

Open Command Prompt as Administrator:

```
secedit /export /cfg C:\SecurityPolicy.txt
```

Open the file and review the settings.

Task 8.2: Generate User Account Report

Create a batch script named `user_audit.bat`:

```
@echo off
echo Password Policy Compliance Report
echo ==================================
echo Generated on: %date% %time%
echo.
echo.
echo Current Password Policy Settings:
echo ---------------------------------
net accounts
echo.
echo.
echo User Account Status:
echo --------------------
net user testuser1
echo.
echo --------------------
net user testuser2
echo.
echo --------------------
net user testuser3
echo.
```

Run the script:

```
user_audit.bat > compliance_report.txt
```

Task 8.3: Document Policy Settings

Create a summary table in your report:

Policy Setting	Required Value	Configured Value	Status
Minimum password length	[MIN_LENGTH]		
Password complexity	Enabled		
Password history	[HISTORY_COUNT]		
Maximum password age	[MAX_AGE]		
Minimum password age	[MIN_AGE]		
Account lockout threshold	[LOCKOUT_THRESHOLD]		
Lockout duration	[LOCKOUT_DURATION]		
Reset lockout counter	[RESET_COUNTER]		

Deliverable:

- SecurityPolicy.txt file
- compliance_report.txt file
- Completed summary table verifying all settings match requirements

Deliverables Checklist

Submit a lab report containing:

1. □ Initial security policy documentation (Part 1)
2. □ Test user creation verification (Part 2)
3. □ Configured password policy screenshots (Part 3)
4. □ Password complexity testing results with explanations (Part 4)
5. □ Configured account lockout policy screenshots (Part 5)
6. □ Account lockout demonstration with Event Viewer (Part 6)
7. □ Password history testing results (Part 7)
8. □ Complete compliance report with summary table (Part 8)
9. □ Reflection: Discuss how these policies align with security best practices and why each setting is important for organizational security

Assessment Rubric

Criteria	**Points**
Password policies correctly configured with required values	20
Account lockout policies properly implemented	20
Password complexity testing completed with analysis	15
Account lockout successfully demonstrated	15
Password history prevention verified	10
Compliance report generated and accurate	10
Documentation quality, screenshots, and explanations	10
Total	**100**

Challenge Questions (Optional Bonus)

1. What security risks exist if `[MIN_AGE]` is set to 0 days? Explain with an example.
2. Why is it important that "Store passwords using reversible encryption" remains disabled?
3. If a user changes their password **[HISTORY_COUNT] + 1** times in one day, can they reuse their original password? Why or why not? (Consider the `[MIN_AGE]` setting)
4. Your company has 100 employees. A user calls saying they're locked out. You check and see 15 lockout events in the past hour across different accounts. What might this indicate?
5. Research and explain the difference between Local Security Policy and Group Policy in a domain environment. When would each be used?

Troubleshooting Tips

Issue: Cannot open Local Security Policy (`secpol.msc`)
Solution: Ensure you're using Windows 10 Pro or Enterprise. Home edition does not include this tool. Verify you have Administrator privileges.

Issue: `gpupdate /force` shows errors
Solution: Run Command Prompt as Administrator. Close Local Security Policy editor before running gpupdate.

Issue: Password complexity not enforcing after configuration
Solution: Ensure `gpupdate /force` was executed successfully. Try restarting the computer.

Issue: Cannot view Event Viewer security logs
Solution: Run Event Viewer as Administrator. If still no logs, security auditing may need to be enabled.

Issue: Account remains locked after lockout duration
Solution: Verify the lockout duration time has fully elapsed. Check system clock. Manually unlock using `net user [username] /active:yes`

Understanding the Placeholder Values

Before implementing the policy, you must understand what each placeholder represents:

- **[MIN_LENGTH]**: Minimum number of characters required in passwords
- **[HISTORY_COUNT]**: How many previous passwords Windows remembers
- **[MIN_AGE]**: Minimum days before a user can change their password again
- **[MAX_AGE]**: Maximum days before user must change password
- **[LOCKOUT_THRESHOLD]**: Number of failed login attempts before lockout
- **[LOCKOUT_DURATION]**: Minutes the account stays locked
- **[RESET_COUNTER]**: Minutes before failed attempt counter resets
- **[USERNAME]**: The name of the user account you're working with
- **[NEW_PASSWORD]**: The password you're attempting to set

Important: Do not use the placeholders literally in commands. Replace them with the actual values provided by your instructor or required by the policy.

Additional Resources

- Microsoft Documentation: Password Policy Settings
- Microsoft Documentation: Account Lockout Policy
- Windows Event IDs for Security Auditing
- `net user` command reference: Type `net user /?` in Command Prompt