Lab Report
___

Your Performance

Your Score: 0 of 7 (0%)   Pass Status: Not Passed

Elapsed Time: 2 minutes 29 seconds   Required Score: 100%

Task Summary

✖ Reset account lockout counter after 60 minutes

✖ Minimum password length 14 characters

✖ Minimum password age 1 day

✖ Enforce password history for 24 passwords

✖ Event log retention set not to overwrite events   Hide Details

> 🟥 Application log
> 🟥 Security log
> 🟥 System log

✖ DCOM Server Process Launcher service disabled

✖ Task Scheduler service disabled

Explanation

In this lab, you use Group Policy Management to configure the default domain policy with the following settings to remediate the issues identified in the vulnerability report:

Policy	Setting
Reset account lockout counter after	60 Minutes
Minimum password length	14 Characters
Minimum password age	1 Day
Enforce password history	24 Passwords
Retention method for application log	Do not overwrite events (clear log manually)
Retention method for security log	Do not overwrite events (clear log manually)
Retention method for system log	Do not overwrite events (clear log manually)
DCOM Server Process Launcher	Disabled
Task Scheduler	Disabled

Complete this lab as follows:

1. Run a Security Evaluator report as follows:
    a. From the taskbar, open **Security Evaluator**.
    b. Next to Local Machine, select the **Target** icon to select a new target.
    c. Select **Domain Controller**.
    d. From the Domain Controller drop-down list, select **CorpDC** as the target.
    e. Click **OK**.
    f. Select the **Status refresh icon** to run the security evaluation.
    g. Review the results to determine which issues you need to resolve on CorpDC.
2. From the top menu, select **Floor 1**.

3. Select **CorpDC**.
4. Remediate password issues in Account Policies as follows:
     a. From Server Manager, select **Tools** > **Group Policy Management**.
     b. Expand **Forest: CorpNet.com** > **Domains** > **CorpNet.com**.
     c. Right-click **Default Domain Policy** and select **Edit**.
     d. Under Computer Configuration, expand **Policies** > **Windows Settings** > **Security Settings** > **Account Policy**.
     e. Select **Account Lockout Policy**.
     f. In the right pane, right-click the *policy* and select **Properties**.
     g. Select **Define this policy setting**.
     h. Enter **60** minutes; then click **OK**.
     i. In the left pane, select **Password Policy**.
     j. In the right pane, right-click the *policy* and select **Properties**.
     k. Select **Define this policy setting**.
     l. Enter the *password setting*; then click **OK**.
     m. Repeat steps 4j–4l for each additional policy.

5. Remediate Event Log issues as follows:
     a. In the left pane, select **Event Log**.
     b. In the right pane, right-click the *policy* and select **Properties**.
     c. Select **Define this policy setting**.
     d. Select the retention method; then select **OK**.
     e. Repeat steps 5b–5d for each additional policy.

6. Remediate System Services issues as follows:
     a. In the left pane, select **System Services**.
     b. In the right pane, right-click the *policy* and select **Properties**.
     c. Select **Define this policy setting**.
     d. Make sure **Disabled** is selected; then click **OK**.
     e. Repeat steps 6b–6d for each additional policy.

7. Verify that all the issues were resolved using the Security Evaluator feature on the ITAdmin computer as follows:
     a. From the top menu, select **Floor 1**.
     b. Select **ITAdmin**.
     c. In Security Evaluator, select **Status refresh** to rerun the security evaluation.
     d. If you still see unresolved issues, select **Floor 1**, navigate to **CorpDC,** and remediate any remaining issues.