11.4.9 Scan for Domain Controller Vulnerabilities

Your Performance

Your Score: 0 of 7 (0%)
Pass Status: **Not Passed**
Elapsed Time: 32 seconds
Required Score: 100%

Task Summary

Required Actions

- ✗ Reset account lockout counter after 60 minutes
- ✗ Use a minimum password length of 14 characters
- ✗ Use a minimum password age of one day
- ✗ Enforce password history for 24 passwords
- ✗ Event log retention set not to overwrite events Show Details
- ✗ DCOM Server Process Launcher service disabled
- ✗ Task Scheduler service disabled

Explanation

While completing this lab, use the following information:

Area	Policy	Setting
Password Policy	Enforce password history	**24 Passwords**
	Minimum password age	**1 Day**
	Minimum password length	**14 Characters**
Account Lockout Policy	Reset account lockout counter after	**60 Minutes**
Event Log	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)**
System Services	DCOM Server Process Launcher	**Disabled**
	Task Scheduler	**Disabled**

Complete this lab as follows:

1. Run a Security Evaluator report.
   a. From the taskbar, open **Security Evaluator**.
   b. Next to Target: Local Machine, select the **Target** icon to select a target.
   c. Select **Domain Controller**.
   d. Using the Domain Controller drop-down list, select **CorpDC** as the target.

e. Select **OK**.
f. Next to Status: No Results, select the **Status Run/Rerun Security Evaluation** icon.
g. Review the results to determine which issues you need to resolve on CorpDC.

2. Access the CorpDC server.
   a. From the top navigation tabs, select **Floor 1**.
   b. Under Networking Closet, select **CorpDC**.

   If you need to return to the ITAdmin computer to review the Security Evaluator results:
   1. From the top navigation tabs, select **Floor 1**.
   2. Under IT Administration, select **ITAdmin**.

3. Access and edit the **CorpNet.local Default Domain Policy**.
   a. From Server Manager, select **Tools** > **Group Policy Management**.
   b. Maximize the window for easier viewing.
   c. Expand **Forest: CorpNet.local** > **Domains** >**CorpNet.local**.
   d. Right-click **Default Domain Policy** and then select **Edit**.
   e. Maximize the window for easier viewing.
4. Remediate the password policy issues in **Account Policies**.
   a. Under Computer Configuration, expand **Policies** > **Windows Settings** > **Security Settings** > **Account Policies**.
   b. From the left pane, select **Password Policy**.
   c. From the right pane, double-click the ***policy***.
   d. Select **Define this policy setting**.
   e. Enter the ***password setting*** and then select **OK**.
   f. Repeat steps 4c-4e for each additional password policy.
5. Remediate the reset account lockout counter issue in **Account Policies**.
   a. From the left pane, select **Account Lockout Policy**.
   b. From the right pane, double-click **Reset account lockout counter after**.
   c. Select **Define this policy setting**.
   d. Enter **60** minutes and then select **OK**.
6. Remediate the Event Log issues.
   a. From the left pane, select **Event Log**.
   b. From the right pane, double-click the ***policy***.
   c. Select **Define this policy setting**.
   d. Select **Do not overwrite events (clear log manually)** and then select **OK**.
   e. Repeat steps 6b–6d for each additional Event Log policy.
7. Remediate System Services issues.
   a. From the left pane, select **System Services**.
   b. From the right pane, double-click the ***policy***.
   c. Select **Define this policy setting**.
   d. Make sure **Disabled** is selected and then select **OK**.
   e. Repeat steps 7b-7d for the remaining System Services policy.
8. Verify that all the issues were resolved using the Security Evaluator feature on the ITAdmin computer.
   a. From the top navigation tabs, select **Floor 1**.
   b. Under IT Administration, select **ITAdmin**.
   c. From Security Evaluator, select the **Status Run/Rerun Security Evaluation** icon to rerun the security evaluation.
   d. If you still see unresolved issues, select **Floor 1**, navigate to **CorpDC**, and remediate any remaining issues.
