Practical 6A – Windows Server Security Features

Lab Requirements:

a) Windows Server NYP-DC1

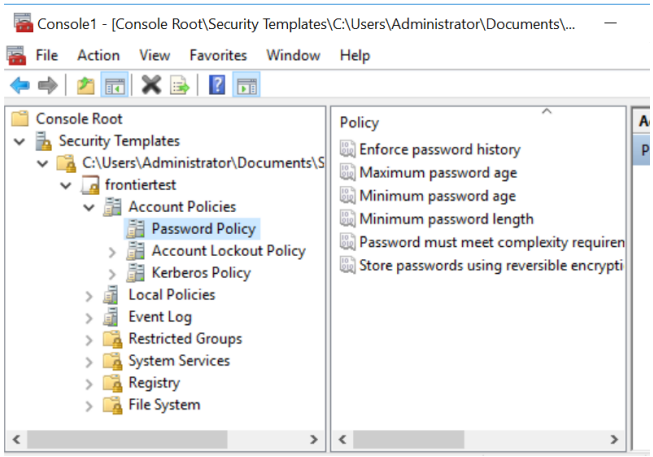
Practice 1

Objectives:

1. Define a new security template to meet custom requirements.

Tasks:

1. Login to NYP-DC1 as administrator and run the **MMC** (type mmc in the run command box). Add the **Security Templates** snap-in.
2. In the MMC with the Security Templates snap-in added, right-click **C:\Users\Administrator\.....** and click **New Template**.
3. In the Template name text box, type **frontiertest**. In the Description text box, type Test security template for the frontier.net domain. Click **OK**.
4. Browse through the configuration settings of the new frontiertest security template. Notice that because the template is new, no settings have yet been configured.
5. Click the triangular sign (I>) next to the frontiertest template to expand it, click the triangular sign (I>) next to **Account Policies** to expand it, click **Password Policy**, and configure the following settings:
    a. Enforce password history – 5 passwords remembered
    b. Maximum password age – 20 days
    c. Minimum password age – 19 days
    d. Minimum password length – 6 characters
    e. Password must meet complexity requirements - Enabled
6. Click on **Account Lockout Policy** and then configure the following settings:
    a. Account lockout duration – 30 minutes
    b. Account lockout threshold – 3 invalid logon attempts
    c. Reset account lockout counter after – 30 minutes



7. Right-click the frontiertest security template and click **Save**. Close the MMC. Click **No** in the Microsoft Management Console dialog box.
8. Open File Explorer and browse to **C:\users\administrator\documents\security\templates**. Double-click the **frontiertest.inf** file to open it in a text editor. Notice that the settings originally configured in the Security Templates tool now appear in the text file.
9. Close the forntiertest.inf file, and then close all windows.

Practice 2

Objectives:

1. Deploy security template settings using Group Policy.

Tasks:

1. Login to NYP-DC1 as Administrator.
2. Open **Server Manager → Tools → Group Policy Management.**
3. Expand the frontier.net icon and right-click on **Default Domain Policy** and select **Edit.**
4. In the **Computer Configuration** section, click the triangular sign (I>) next to **Policies → Windows Settings** to expand it.
5. Explore the **Account Policies → Password Policies and Account Lockout Policies** and note their settings before the next step.
6. Right-click **Security Settings** and click **Import Policy**.
7. In the Import Policy From window, click **frontiertest.inf** and click **Open**.
8. After importing the security template settings to the Default Domain Policy, expand **Account Policies** and browse through the **Password Policy** and **Account Lockout Policy** sections. Verify that the settings from the frontiertest security template have been imported into the GPO.
9. Close the Group Policy Management Editor window, as well as the properties of the frontier.net domain.

Practice 3

Objectives:

1. Use the Security Configuration and Analysis tool to compare Group Policy and security template settings.

Tasks:

1. Login to NYP-DC1 as Administrator.
2. Open a new **MMC** and add the **Security Configuration and Analysis** snap-in.
3. Right-click the Security Configuration and Analysis icon and click **Open Database**.
4. In the Open database window, type **SecurityTest** in the File name text box and then click **Open**.
5. In the Import Template window, click **frontiertest.inf** and click **Open**.
6. Right-click the **Security Configuration and Analysis** icon and click **Analyze Computer Now**.
7. In the Perform Analysis dialog box, click **OK** to accept the default log file location. The Analyzing System Security dialog box opens.
8. Click the triangular sign (I>) next to Security Configuration and Analysis → **Account Policies** to expand them, and then click **Password Policy**.
9. Review both the Database Setting column and the Computer Setting column. The first column outlines the settings found in the database that relate to the template, whereas the second column outlines the settings currently configured on your server. Note that the icons displayed as part of each setting outline whether or not your server's current configuration meets or exceeds the settings outlined in the security database.
10. As time permits browse through additional settings such as those found in the Account Lockout Policy, User Rights Assignment, and Security Options sections.
11. Right-click **Security Configuration and Analysis** and select **Configure Computer Now…** Click **OK** for the dialogue boxes that follow. Repeat steps 6 to 9 above. What happened? (the Database Setting and Computer Setting should be in sync).
12. Close the MMC without saving any changes.

Practice 4

Objectives:

1. Explore the default audit settings configured on a Windows Server domain controller.

Tasks:

1. Login to NYP-DC1 as Administrator.
2. Open **Server Manager → Tools → Group Policy Management**.
3. Click on **Domain Controllers** and right-click the **Default Domain Controllers Policy** and click **Edit**.
4. In the **Computer Configuration** section, click the triangular sign (I>) next to **Policies → Windows Settings → Security Settings → Local Policies** to expand them.
5. Click the **Audit Policy** node to view its contents. Notice the policy settings and their configured default values in the Policy Setting column.
6. Double-click the **Audit account logon events** icon to view its configured settings. What is their default setting? _____

7. Browse through additional policy settings as time permits, but make no changes.

Practice 5

Objectives:

1. Configure and test new audit policy settings.

Tasks:

1. Continue from previous practice.
2. Use **Group Policy Management** to open and view the settings of the **Default Domain Controllers Policy** GPO auditing settings.
3. Double-click the **Audit account logon events** icon to view its properties.
4. In the **Audit account logon events** section, check the **Define these policy settings** and click both the **Success and Failure** check boxes and click **OK**. (Computer Configuration → Policies → Windows Settings → Security Settings →Local Policies → Audit Policy)
5. Double-click the **Audit object access** icon to view its properties (click the Explain tab to view the details).
6. In the Audit object access section, check the **Define these policy settings** and click both the **Success and Failure** check boxes and click **OK**.
7. Close all the opened windows.
8. Open a Command Prompt (Admin) and type **gpupdate /force** then press **Enter**.
9. Log off from NYP-DC1.
10. Attempt to login NYP-DC1 as Administrator with a **wrong** password. This logon attempt fails.
11. Log on as the user Administrator with correct password.
12. Click **Server Manager → Tools → Event Viewer**.
13. Click the **Windows Logs → Security** icon to view the contents of the security log.
14. Search through the security log for a Failure event in category Account Logon that uses the event ID number **4771**. Double-click this Failure event to open it and view its details.
15. Read through the information provided by the event and then close all open windows.

Practice 6

Objectives:

1. Audit failed and successful access to an NTFS folder.

Tasks:

1. Login to NYP-DC1 as administrator.

2. Create a new folder called **Accounting** in any drive. Secure this folder with NTFS permissions such that only the **Administrators** group account have **Full Control** of the folder (remove others and leave only System group and Administrators group). Leave the properties dialog box of the folder open once complete.
3. On the Security tab, click the **Advanced** button, and then click the **Auditing** tab.
4. Click the **Add** button. Click **Select a principal** and type **Everyone** in the Enter the object name to select text box → **Check Name** → and click **OK**.
5. In the **Type** box, you can select **All**, **Success** or **Fail**. Select **Fail**.
6. Under Basic permissions:, accept the default settings (Read & execute, List, Read).
7. Click **OK** → **OK**.
8. Click **OK** to exit the Accounting Properties window.
9. Log off and then log back on using the **user1-marketing** user account with the password Pa$$w0rd (if user1-marketing cannot login to NYP-DC1, add it to the Backup Operators group first).
10. Open Windows Explorer and browse to drive and then attempt to open the **Accounting** folder. Access should be denied according to the NTFS permissions configured in Step 2.
11. Try to delete the Accounting folder.
12. Log off and then log back on using the **Administrator** account.
13. Click **Server Manager → Tools → Event Viewer.** Expand it to open **Windows Logs → Security** icon to view its contents. Search for **Failure** events.
14. View the Details of the events to see the failed attempts by user1-marketing.
15. Close all open windows.

Practice 7

Objectives:

1. Edit security log settings and save events for archiving purposes.

Tasks:

1. Login to NYP-DC1 as Administrator.
2. Click **Server Manager →Tools → Event Viewer**.
3. In **Windows Logs → Security,** click **Properties** in the Right panel.
4. Type **250000** in the Maximum log size text box.
5. In the When maximum log size is reached section, click the **Do not overwrite events (Clear logs manually)** radio button and then click **OK**.
6. A message appears telling you that the log file size must be an increment of 64K. Click **OK** to continue.
7. Right-Click the **Security** icon and select **Save All Events As…**.
8. In the File name text box, type seclog-MM-DD-YY using today's date for the filename variables.
9. Click the **Save as type** list arrow to view the different formats in which a log file can be saved. On this list, click Event Log (*.evt), and then click the Save button.

10. Note that the security log events are not cleared as part of a save operation. It's worth noting that you are prompted to save events when you attempt to clear an event log.
11. Right-click the Security icon and click **Clear log** all Events. This empties the security log with the exception of any new events.
12. Right-click the Security node and click **Open Saved Log**. Click the log file saved in Step 7 and then click Security in the Log Type list box. Click **Open**. Notice that the contents of the saved log now appear in the security log.
13. Close all open windows.

[THE END]