Name: _____

Date Started: _____

Date Finished: _____

LAB 3: Analyzing Security Configuration

Objectives:

STEP 1. Power up the VM
STEP 2: Create an Enterprise Admins
STEP 3. Verify user is a member of the Enterprise Admins Group.

Requirements:

1. *Screen shots all the windows configuration from Step 1 to Step 3.*
2. *Label the necessary result in the configuration.*
3. *Display the Final Result for each Steps.*

Background / Scenario

Security Templates contains over 250 security policies (for example, Account lockout duration), and that does not include the thousands of custom settings that an administrator can configure in the Restricted Groups, Registry, and File System nodes. Obviously, it would be impractical for administrators to manually investigate each setting on each computer to determine whether any setting was correctly configured.

Fortunately, the Security Configuration and Analysis tool allows administrators to verify security policy compliance in a few minutes. There are various results for various settings.

If the security template does not define a configuration for a setting, "Not Defined" is displayed in the Database Setting column, for example. The Security Configuration and Analysis tool displays a red icon when there is a conflict between the settings of the database and the computer; a green icon indicates that the database and computer settings match. In this lab, you perform an analysis that compares your server's settings to the security template you created in Lab 1.

Note: You will need installation privileges and some knowledge of the process to install Windows server 2012 R2.

Required Resources

- PC
- VM Virtual Manager
- Windows Server 2012 R2
- Successful completion of Lab 1.

STEP 1. Power up the VM

1. Power the Virtual Box by clicking Start, then run the Server.

2. Click the Start window, log in to Administrator and provide the Password

STEP 2: Create an Enterprise Admins

In this lab, you create a domain user account of your security template created in your Lab 1.

1. Click Ctrl Del, Log into the Server Administrator, then provide the password. You land on the Server Manager Dashboard.

2. In Server Manager, click Tools, then click Active Directory Users and Computers, and expand your domain (starzy.local).

3. Right-click the Users container, select New, and then select User.

4. Configure the new user as follows: First name: Lee, Initial: F, Last name: Ko, User logon name: leefko. Click Next.

5. In the Password box, enter Pa$$word and repeat this in the Confirm password box.

6. Remove the check from User must change password at next logon box, click Next, and then click Finish.

7. Verify the new user's group membership by doing the following: If necessary, click the Users container to display its contents in the right pane, right-click the Lee F. Ko account in the right pane, and select Properties.

8. Click the Member Of tab, verify that Lee Ko is a member of the Domain Users group only, and click Cancel.

9. Verify the membership of the Enterprise Admins group by doing the following: Double-click the Enterprise Admins group in the right pane, select the Members tab,

verify that the user, Administrator, is the only member of the group, and click Cancel. Close the Active Directory Users and Computers console.

10. Return to the Security Configuration and Templates console you created in your Lab 1 expand the Templates folder in the left pane, and select Restricted Enterprise Admins Group in the left pane to reveal its policies in the middle pane.

11. Double-click the Restricted Groups node, right-click anywhere in the white area of the right pane, and select Add Group.

12. In the Add Group window, click Browse. In the Select Groups window, type Enterprise in the Enter the object names to select box, and then click Check Names.

13. In the Multiple Names Found window, select Enterprise Admins and click OK. In the Select Groups window, Enterprise Admins should appear underlined. Click OK, and in the Add Group window, click OK.

14. In the Enterprise Admins Properties window, click Add Members.

15. Next, select the only accounts that should be in the Enterprise Admins group. In the Member window, click Browse. In the Select Users, Service Accounts, or Groups win type Administrator in the Enter the object names to select box, then click Check Names the Administrator account should appear underlined. Click OK, click OK in the Member window, and click OK in the Enterprise Admins Properties window. You have configured this security template to assure that only the Administrator is a member the Enterprise Admins group. However, this is only an available template; it has not been applied to your server.

15. Close the Security Configuration and Templates console. If prompted, click Yes to save the console settings, and log off

STEP 3. Verify user is a member of the Enterprise Admins Group.

1. Log on to Server as Administrator. In the Server Manager, click Tools, then click the Active Directory Users and Computers console.

2. Click the Users container, right-click the account of Lee F. Ko, and select Add to a group.

3. Type Enterprise Admins and click Check Names. When the Enterprise Admins group appears underlined, click OK.

4. Click OK in the Active Directory Domain Services window.

5. Verify that Lee Ko is a member of the Enterprise Admins group by doing the following: Double-click the Enterprise Admins group, click the Members tab and click OK. Close Active Directory Users and Computers.

6. Open the Security Configuration and Templates console made earlier.

7. Right-click Security Templates, select New Template Search Path, navigate to C:\Users \Administrator\Documents \Security, select the Templates directory, and click OK.

8. Right-click Security Configuration and Analysis in the left pane under the Console Root and select Open Database.

9. If necessary, navigate to C: Users\Administrator \Documents \Security \Database, type EnterpriseAdminGroupRestrict in the File name box, and click Open. This is a new database of security settings that you are creating and against which you will compare your server's current settings. Note that you have automatically switched to the Templates folder so that you can select a template.

10. Select the Restricted Enterprise Admins Group that you made earlier and click Open.

Now the database against which you will compare your server's current settings is the same as the template you made earlier that restricts the membership of the Enterprise

Admins group.

11. Right-click Security Configuration and Analysis, select Analyze Computer Now, and click OK to accept the Error log file path.

12. When the analysis is complete, expand the Security Configuration and Analysis node and click Restricted Groups.

13. Notice the red circle with the "X" inside it, which indicates that the server's current configuration is inconsistent with the settings in the Restricted Enterprise Admins Group security template.

14. Double-click the Enterprise Admins group listing that has the red error icon to see the associated properties.

15. Notice that the Database Setting indicates that leefko is not supposed to be in the Enterprise Admins group.

16. Click Ok to close the Enterprise Admins Properties dialog box, close the Security Configuration and Templates console, click Yes to save the console settings, and click OK to accept the path if prompted.

17. Close all windows and log off.