Name: _____

Date Started: _____

Date Finished: _____

LAB 4: Applying Security Settings with Auditing Object Access

Objectives:

STEP 1. Power up the VM
STEP 2: Create a Security Settings from a Security Template and Verifying System Compliance.
STEP 3: Auditing Object Access

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

Servers do not generally fall out of compliance with security policy requirements by the selves. Although file corruption or memory errors could theoretically cause these settings change, it is usually the actions of server administrators that result in alterations of security settings. Sometimes, software installation requires temporary changes in registry permissions. The application of updates and patches can also require temporary changes in security settings. Whatever the reason for deviations from the required security setting, the serve administrator is the person to assure that the server is in compliance with security policy requirements. Using the Security Configuration and Analysis console, administrator's car both audit the compliance of their servers and apply the required settings with a few mouse clicks.

Hardening a server generally involves keeping current with updates and patches, removing unneeded services and user accounts, and so on. Another important task, especially if the server is on the demilitarized zone (DMZ), is to configure logging of authentication attempts, service events, and users' access of

resources. Of course, logging itself is not enough; the log files need to be reviewed regularly.

> **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 2.

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 a Security Settings from a Security Template and Verifying System Compliance

In this lab, you apply setting from a security template to a server and then verify that it is completed successfully.

1. Open the Security Configuration and Templates console made in Lab 1.

2. Right-click Security Configuration and Analysis in the left pane under Console Root.

Select Configure Computer Now and click OK to accept the Error log file path.

3. When the configuration is complete, right-click the Security Configuration and Analysis node, click Analyze Computer Now, and click OK to accept the Error log file path.

4. Click the Restricted Groups node under Security Configuration and Analysis. Notice that there is now a green circle with the white check mark inside it, which indicates that the server's current configuration for this setting is now consistent with the settings in the Restricted Enterprise Admins Group security template.

5. Double-click the Enterprise Admins group listing and verify that the server's settings and the database settings are compliant. Note that the lee account is no longer listed as being in the Enterprise Admins group. Close the Enterprise Admins

Properties window, close the Security Configuration and Templates console, and save the console settings if prompted.

6. Does Lee Ko still have Enterprise Admin privileges on your server? Verify your answer by doing the following to examine Active Directory Users and Computers: Click Start, click Administrative Tools, and open Active Directory Users and Computers.

7. Open the Users container, double-click Lee Ko account, and click the Member Of tab. The Restricted Groups setting that you had configured in the security template has been applied to the server, and it has enforced the setting that states only the Administrator can be a member of the Enterprise Admins group.

8. Close all windows and log off.

STEP 3: Auditing Object Access

You configure auditing.

1. Log on to Server as Administrator.

2. Click File Explorer, then double-click Local Disk (C:).

3. In the right pane, right-click in a blank area and select New, click Folder, and name the folder Sales.

4. Open Sales. In the right pane, right-click in a blank area and select New, click Text Document, and name the document Sales Report.

5. Open Sales Report and enter the following text: Please enter your sales estimates for this quarter to Php100,000.

6. From the File menu, select Exit and click Save.

7. Close the Sales window,

8. Click Tools, and double-click Active Directory Users and Computers. If necessary, expand your domain (starzy.local), right-click the Users container, click New, click User, and create two users configured as shown in Table 4-1.

Full Name	User Logon name	Password	User must change password at Next Logon
Rain F. Tree	raintree	Pa$$word!	Unchecked
Brain T. Wash	brainwash	Pa$$word!	Unchecked

9. Right- click the Users container, Click New, and click Group. Verify that the Group scope is set to Global and that the Group type is set to Security. In the Group name

box, type Sales Managers and click OK. Repeat the procedure to create a second global security group named Sales Associates.

10. Double-click the Sales Managers group, click the Members tab, and click the Add but-ton. In the Enter the object names to select box, type Richard and click the Check Names button. When the Rain F. Tree account appears underlined, click OK, then click OK on the Sales Managers Properties window. Repeat this procedure to make Brain T. Wash a member of the Sales Associates global group, and then close Active Directory Users and Computers.

11. Click File Explorer, then double-click Computer, open Local Disk (C), right-click the Sales directory, click Properties, click the Security tab, click Edit, select the Users group, and click Remove. Read the error message that appears. Inheritance of permissions set at the root of C: must be blocked before you can remove the Users group.

12. Click OK on the error message and close the Permissions window. In the Sales Properties window, click the Advanced button. In the Advanced Security Settings for Sales window, click the Disable inheritance button, click the convert inherited permissions into explicit permissions on this object option, click OK in the Advanced Security Settings for Sales window, and click OK again.

13. In the Sales Properties window, click Edit, select the Users group, and click Remove.

Click the Add button. In the Enter the object names to select box, type Sales, and then click Check Names. Holding the Ctrl key, select both the Sales Associates and Sales Managers groups, release the Ctrl key, and click OK.

Click OK in the Select Users, Computers, Service Accounts or Groups window. In the Permissions for Sales window, select Sales Associates and check the Full control box in the Allow column. Sales Associates should now have Full control, Modify, Read & execute, List folder contents, Read, and Write checked.

14. Click Sales Managers and verify that they have only Read & execute, List folder contents, and Read checked. Note that members of the Sales Managers group will be able to read documents in the Sales folder but will not be allowed to write to the files or directory or delete anything in it. Click OK in the Permissions for Sales window, and click OK in the Sales Properties window.

15. In order to allow nonadministrative accounts to log on locally to the domain controller so that you can test the new user's permissions, do the following: in Server Manager, click Tools, double-click Group Policy Management, expand the Forest, expand Domains, expand your domain, expand the Domain Controllers, right-click the Default Domain Controllers Policy, and click Edit.

16. Under Computer Configuration, expand Policies, expand Windows Settings, expand Security Settings, expand Local Policies, and click User Rights Assignment. In the right pane, double click the policy Allow log on locally, and click Add User or Group. In the Add User or Group window, click Browse, and in the Enter the object names to select box, type Domain, click Check Names, select Domain Users, click OK, and click OK three more times. Now, domain users can log on to your domain controller interactively instead of just over the network.

17. In the left pane, click Audit Policy. In the right pane, double-click Audit object access, place a check mark in the Define these policy settings box, place a check mark in the Failure box, and click OK. Close Group Policy Management Editor and Group Policy Management.

18. Open a command prompt, and enter gpupdate /force. Now, the policies that allow Domain Users to log on locally to the domain controller and that enable auditing of object access are activated. They would have updated automatically within 5 minutes-the default time for domain controllers to refresh their policies. However, enabling audit access does not mean that we can track accesses to the Sales folder yet. We have to set auditing on each object we want to track. If setting the policy to audit object access resulted in all system objects being audited, the system would bog down and stop because of all the logging being done. Close the command prompt.

19. Enable auditing of object access on the Sales folder as follows: right-click C:\Sales, click

Properties, click the Security tab, click Advanced, and click the Auditing tab.

20. In the Advanced Security Settings for Sales, click the Add button. Click Select a principal.

In the Enter the object name to select box, type Everyone, click Check Names, and when the Everyone group appears underlined, click OK.

21. The Auditing Entry for Sales window appears. Select the Fail option from the Type drop down list in the top portion of the window, then click Show advanced properties, and place check marks in the boxes for Create files / write data, Delete subfolders and files, and Delete. Click OK three times to complete auditing configuration on the Sales folder. Close all windows and log off.

22. Log on as brainwash. Click File Explorer, double-click Computer, double-click Local Disk (C:), open the Sales folder, open Sales Report, and add this line: These figures are due Monday, April 20th. Save the file, close all windows, and log out.

23. Log on as raintree. Click File Explorer, double-click Computer, double-click Local Disk (C), open the Sales folder, open Sales Report, and add this line: Please include sales from accounts that have closed. Save the file. What happens? Assume

that you have logged in as a regular user and that you do not know the administrative password. Cancel the attempt to save the file. Try to delete the Sales Report document.

Cancel the attempt to delete the file. Try to delete the Sales folder. Close all windows and log out.

24. Log on as Administrator. In Server Manager, click Tools, then select Event Viewer, expand Windows Logs, and click Security. There are likely to be a lot of events. The logged events that have a key icon indicate successful actions. Those with padlocks indicate an account's failed attempts to perform a prohibited action. In the Actions pane on the right, click Filter Current Log. Click the drop-down arrow in the Logged box, select Last hour, and click OK. You will need to scroll down in the upper window to see what object was accessed (the folder or file) and what action was attempted (delete).

Explore the failure events by double-clicking them and find evidence that Rain Tree attempted to write to the Sales Report file, attempted to delete the Sales Report file, and attempted to delete the Sales folder.

25. Close all windows and log off.

1. Explain the attempt of Rain Tree why he cannot delete any files. What happens?