For this lab:

## Discuss:

* What the hardest part of the lab was and why you thought it was hard
* Any problems you had with the lab and what was done to fix the issues (even if the instructor fixed the issue. Pay attention!)
* Improvements you would make to the lab (Two minimum)

## Questions to answer (Answer the following questions in the discussion section of your lab report):

* Why or why not did the group policy prevent [FTP.EXE](ftp://FTP.EXE) from working?
* In this lab, auditing was turned on for object access. Where else must auditing be turned on for file and folder access events (open a file, read a file, delete a file, etc) to be recorded in the security event log?
* Did the Screen Lock Policy work for your administrative user?
* If not, why not?
* If it didn’t work, what could be done to make sure that the Screen Lock Policy worked?
* Did the “Deny Apply group policy” setting for the test user/NoScreenSaver group work as expected?
* If not, why not?
* If it didn’t work, what could be done to make sure that the NoScreenSaver group has no screen saver set?

## Screenshots to include

1. A screenshot of the domain password policy
2. A screenshot of the FTP software restriction policy.
3. A screenshot of what happened when you tried running the FTP command

## Things to include in the lab report in an Appendix at the end:

1. Group Policy results report for the test user. To get this report, right-click on Group Policy results in the Group Policy Management console.
   1. Select “Group policy results wizard. . .”
   2. Click Next twice (past the Select computer screen).
   3. On the User Selection page, select “Select a specific user” and choose “test” from the list. Click Next twice.
   4. Click Finish
   5. Right-click on the new report and choose Save Report.

# Pre-lab

1. You should have already completed these steps in the first, CORE Lab: Set up a Windows 2008 Domain Controller, install Active Directory, Create and join a Windows 7 PC to the domain, configure the CORE machine for remote management (firewall) Install RSAT.

# LAB

1. Run GPMC. It’s located under Start 🡪 All Programs 🡪 Administrative tools 🡪 Group Policy Management
   1. Browse to the Default Domain Policy (Forest 🡪 Domains 🡪 Your Domain Name 🡪 Group Policy Objects 🡪 Default Domain Policy
      1. Click on the Settings tab and wait for the system to generate the report. Click on the “Show All” button and review all the settings in this policy. Note – you can save this report to a file by right-clicking on the policy and choosing “Save Report. . .” You will need to do this for several policies later in the lab.
2. Right-click on the **Default Domain Policy** and choose Edit
   1. Through looking at your notes and using online searches, you are to configure the following ‘Computer Configuration’ Windows Security settings:
      1. Password policy (**a screenshot of this should appear in the lab report**):
         * Maximum password age should be 31 days
         * Minimum password age should be 2 days
         * Minimum password length should be set to 8 characters
         * Password complexity requirements are to be enabled
      2. Account lockout Policy:
         * Accounts are to be locked out after 3 invalid attempts
         * Lockout duration is to be set to 5 min
         * Reset account lockouts after 5 min
      3. Audit policy:
         * Audit account logon events Success, Failure
         * Audit account management Success, Failure
         * Audit directory service access Failure
         * Audit logon events Success, Failure
         * Audit object access Success, Failure
         * Audit policy change Success, Failure
         * Audit privilege use Success, Failure
         * Audit process tracking Not Defined
         * Audit system events Success, Failure
      4. Security Options: (keep [kb823659](http://support.microsoft.com/kb/823659) handy for this one)
         * Accounts: Rename administrator account to support
         * Interactive logon: Enable Do not display last user name
         * Interactive logon: Message text for users attempting to log on: only authorized users are allowed to log into this system.
         * Interactive logon: Message title for users attempting to log on: Authorized users only!
         * Interactive logon: Prompt user to change password before expiration: 3 days
         * Network security: Enable Do not store LAN Manager hash value on next password change
         * Network security: LAN Manager authentication level: Send NTLMv2 response only\refuse LM
      5. Disable The following service:
         * Themes
      6. Under Administrative Templates 🡪 System 🡪 Removable Storage Access configure the following:
         * All removable Storage classes: Deny all access: Enabled
      7. Software Restriction Policies
         * Create a new policy named BlockSoftware that is linked to the Domain: In the Group Policy Management console, right-click on the Domain name and select “Create and Link GPO Here. . .”. Name the policy “BlockSoftware”
         * In User Configuration 🡪 Policies 🡪 Windows Settings 🡪 Security Settings 🡪 Software Restriction Policies, Right-click Software Restriction Policies and select “New Software Restriction Policies”
         * Right-click Additional Rules and select “New Hash rule. . .”
         * Click on the Browse button. Browse to C:\Windows\system32\ftp.exe and select it.
         * The hash value will be automatically entered along with the file information. The security level should be set to “Disallowed”. Put “disallow client FTP access” in the Description field. And click on “OK” (**You should include a screenshot of this in your lab report**)
   2. Create a new policy named “Lock workstation policy” that is linked to the domain.
      1. Configure the following ‘User Configuration’ Windows Security setting:
         * In the Group Policy Management console, right-click on the Domain name and select “Create and Link GPO Here. . .”. Name the policy “Lock workstation policy”
         * Right-click the Lock workstation policy and Choose Edit. Configure the following settings under User Configuration 🡪 Administrative Templates 🡪 Control Panel 🡪 Display:

* Enable Hide Screen Saver tab
* Enable Password protect the screen saver
* Enable Screen Saver
* Screen Saver executable name scrnsave.scr
* Enable Screen Saver timeout
* Number of seconds to wait to enable the Screen Saver 60
  1. From the command line, run the command “gpupdate /force”
  2. Create a new user named “test” using Active directory users and computers.
  3. Create a new group named “NoScreenSaver”. Add the test user to the NoScreenSaver group.
  4. Log out and back in as the test user.
  5. Log out then back in again as support (your policy should have renamed the administrator account to support)
  6. Create an exception to the screensaver policy
     1. Go back into the Group Policy Management console. Browse to Forest 🡪 Domains 🡪 <your domain>.
     2. Click on the “Lock Workstation policy” and select the “Delegation” tab. Click on the “Advanced. . .” button in the lower right.
     3. Click on the “Add. . .” button and add the NoScreenSaver group.
     4. Change the permissions for the NoScreenSaver Apply Group Policy setting to Deny.
     5. Click on OK. Click on Yes to continue.

1. Check the policy settings (user policy)
   1. While logged in with your “0” administrative account; wait 60 seconds and see if the screen saver policy kicks in (**it should, document this in your lab**).
   2. Log out then log back in again as the test user.
   3. Wait 60 seconds to see if the exception to the screen saver policy worked. **Document what happened in your lab and why you think it happened.**
   4. **Open a CMD prompt and try using the FTP command. Document the results in your lab report, including a screenshot.**

# LAB 2 Evaluation Criteria

NAME: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| COMPONENT | POINTS | | POINTS EARNED | COMMENTS |
| **Overall look and feel** | | | | |
| **Title Page** | 3 |  | | Title page neat, clean, includes lab # and lab title, Student’s name, date, e-mail address, class and section number are included. |
| **Table of Contents** | 2 |  | |  |
| **Executive Summary** | 5 |  | |  |
| **Professional Appearance** | 5 |  | | Professional overall look, font etc – readability spelling and grammar |
| **Header** | 2 |  | | – Lab Title |
| **Footer** | 2 |  | | – page, course # and student name |
| **Section Headings** | 2 |  | |  |
| **Numbered & Labeled Figures** | 2 |  | | Tables, Diagrams, Screenshots etc labeled and numbered |
| **Numbered Pages** | 2 |  | |  |
| **Content** | | | | |
| **Body Content** | 5 |  | | Clear and well organized point by point description of the actions taken  Each component should have its own section. |
| **Tables/Diagrams** | 5 |  | | Any tables and diagrams in 10-point Currier new font, with paragraph shading of White, Background 1, Darker 15% ***. A description must follow each table or diagram, detailing what was going on and why.*** |
| **System Configuration/Reports** | | | | |
| **Proper function of**  **Windows Vista**  **Windows 2008** | 10 |  | | The following configuration is in place:  System is functioning as it should at the end of the lab – Windows 7 can manage the Windows 2008r2 CORE Domain controller . Group policy functioning properly. [FTP.exe](ftp://FTP.exe) blocked correctly. |
| **Questions/Discussion addresses issues brought up in the Lab** | 15 |  | | Systems are properly configured:   * Screenshots included * AD installed correctly * Computers renamed properly * Group policy correctly configured. * Software restriction policy correctly configured |
| **Total:** | 60 |  | | (final total divided by 6 for grade posted in BB) |