***Evidence:***

* Setup TCP/IP Configuration on your Computer
* IP Address : 100.50.25.X/24
* Where : X is your PC HOST
* Create two Organizational Unit(OU):
* Sales1
* Marketing1
* Create two users in both OUs as follows:
* Sales1(OU) : Sales1user1, Sales1user2
* Marketing1(OU): Marketing1user1, Marketing1user2
* Create groups in both OUs as follows:
* Sales1(OU) : Sales1group
* Marketing1(OU): Marketing1group
* Membership:
* Sales1user1 & Sales1user2 are member of Sales1group
* Marketing1user1 & Marketing1user2 are member of Marketing1group
* Create four groups in Users container as follows:
* PasswordAdmin1
* Sales1Admin
* Marketing1Admin
* BackupAdmin1
* Create a user “bulbul” which password will be “Bismillah786 ” & will be a member of BackupAdmin1 group.
* You have to configure the Security of your Directory service as the following requirements:
* **Delegate Control:**

Ensure that members of the specified groups are allowed to perform only the administrative tasks shown in the following table:

|  |  |
| --- | --- |
| Group | Administrative Tasks |
| **PasswordAdmin1** | **Reset Password in the Domain** |
| **Marketing1Admin** | **Full Control in the Marketing1 Organizational unit(OU)** |

* ***Create a GPO, so that Members of Sales1 OU (Sales1 users) cannot access control panel***

***And test the effect by log on interactively to your domain controller.***

* ***Create a security template and save as “ID-Salam ” in default location.***
* ***Set the following policies in your security template & compare or analyze with your current system policies:***
* Password must changed within 50 days
* Remember ten password
* Password must be at least seven characters long
* Password must not be complex
* Account will be locked out for 11 minutes, if three invalid logon attempts occur.
* Users need not require press Ctrl+Alt+Delete to log on
* Users can shut down without having to log on.