Experiment No: 3

Date:

SETTING PERMISSIONS TO USERS

<u>AIM:</u>

To demonstrate the working of user permission settings, by doing the exercise given below.

Create three users X, Y and Z with the following criteria.

- 1. No complex password
- 2. Minimum password length 3
- 3. Password history set to 3
- 4. Lock account on 2 invalid logon
- 5. Lockout duration set to one minute.
- 6. Set permission for the users to logon to the server itself.

Create a folder 'test' in the C drive and set the following permissions.

- 1. $X \rightarrow \text{Read only}$
- 2. $Y \rightarrow Full permission$
- 3. $Z \rightarrow No \text{ permission}$

PROCEDURE

• Changing the Group Policy:

Step 1: Press Win + R to bring out the Run dialog. Then type gpmc.msc and hit the Enter key to open the Group Policy Management Console. (Or go to Server Manager -> Tools -> Group Policy Management).

Step 2: Expand the item **Forest: <your domain>**, then the folder **Domains**, and expand your domain.

Step 3: Go to your domain -> Group Policy Objects -> Default Domain Policy.



Step 4: Right click on it and select Edit.

Step 5: In the new window, expand Computer Configuration -> Policies -> Windows

Settings -> Security Settings -> Account Policies -> Password Policy.



Step 6: In the right pane, you can change the password policy according to your own needs by double clicking each one.



Step 7: Similarly, select Account Lockout Policy to change the account lockout settings.



• Creating User:

Step 1: Open Start Menu and click on "Administrative Tools".

Step 2: Now a list of items will appear; select "Active Directory Users and Computers".

Step 3: Right-click on the domain and go to "New". In New go to the "Users" to add a "New User".

Step 4: Now a form will be available. Then provide all necessary details of the new user. After that click on the "Next" button.

Step 5: Select proper password options. Click Next.

Step 6: Now all the provided values will be shown and will be asked to click on the "Finish" button. Click it to finish the user creation.

• Local Sign-on behavior

By default, a user can't log on to the server system. To change this User Local Sign-on behavior, we have to change the **Default Domain Controllers Policy**.

Step 1: In the Group Policy Management console, go to Default Domain Controllers Policy.

Step 2: Right click on it and select Edit.

Step 3: In the new window, expand Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Local Policies -> User Rights Assignment -> Allow logon locally and add the users who need to logon to the server computer. (To add user/group, double click it. Properties-> Add User or Group -> Browse -> Advanced -> Find Now)

	 ▷ Domain Controllers □ Group Policy Objects □ Default Domain Controllers Pc □ Default Domain Policy 	The following sites, domains, and OUs are linked to this GPO:			
		Dor Dor	main Controllers	No	Yes
<	Group Policy Management Editor				
	File Action View Help				
	Computer Configuration	^	Policy		
	 ✓ Policies ▷ Software Settings ✓ Windows Settings ▷ Name Resolution Policy ⓒ Scripts (Startup/Shutdown) ✓ Security Settings ▷ Account Policies ✓ Local Policies ▷ Audit Policy ☑ User Rights Assignment ▷ ☑ Security Options 		📓 Access Credential Manager as a tru	sted caller	
			Access this computer from the network		
			Act as part of the operating system		
			Add workstations to domain		
			Adjust memory quotas for a proces	55	
			Allow log on locally		
			Allow log on through Remote Desk	top Services	
			Back up files and directories		
		≡	Bypass traverse checking		
			Change the system time		
			Change the time zone		

• Updating the Group Policy

After any policy has been changed, open **Run (Window key + R)** dialog, type **cmd** and hit **Enter** to open **Command Prompt**. Then run the command **gpupdate/force** to update policy.



• Sharing a Folder

Step 1: Create a folder in the desired location

Step 2: Right click and take Properties.

- Step 3: In the tab Sharing, click Share.
- **Step 4:** Select the user and set the desired permissions.

Step 5: If the user has the permission to logon to the server system, the **Security** tab also has to be configured accordingly.

RESULT:

Implemented the given criteria successfully.