Domain GPOs

Introduction and/or Background

Tx Rig is in the final stages of server deployment and is ready to create some Group Policies for their domain.

Objectives

In this project/lab the student will:

- Create and implement Active Directory Group Policy to define the company wide Password Policy applied to all users in the domain
- Configure Authentication Policies for Kerberos, and Account Policy settings, and enable auditing
- Test password GPO by logging to the TxRig domain from your virtual client
- Verify you have a snapshot of your PC in case you need to revert back

Equipment/Supplies Needed

- VMWare Workstation Pro
- Windows Server 2019 Virtual Machine

Assessment Criteria

- Proof Accounting Password Policy Settings (PrtScr #1)
- Proof Lockout Policy Settings (PrtScr #2)
- Proof of Kerberos Policy Settings (PrtScr #3)
- Proof of Event Log Retention for Security, System, and Application logs (PrtScr#4)
- Proof of Client lock out – client side (PrtScr #5)
- Answers to the Reflection questions in a text file

Assignment

Part 1: Creating Group Policy Object

1. Open Server Manager, Tools, Group Policy Management *Note: Group Policy Management was automatically installed with the install of Active Directory*

2. Expand Forest TxRig_your initials, Double click Default Domains GPO, view Settings tab. It might take a minute or two to open the report. Click **Show All** to view all current settings that are defined for this domain
3. Scroll down to Computer Configuration, view default "Account Policies / Password Policy located under policies, windows settings, security settings to view current policies that are set.

Part 2: Configure Domain Wide Account, Authentication, and Audit Policies

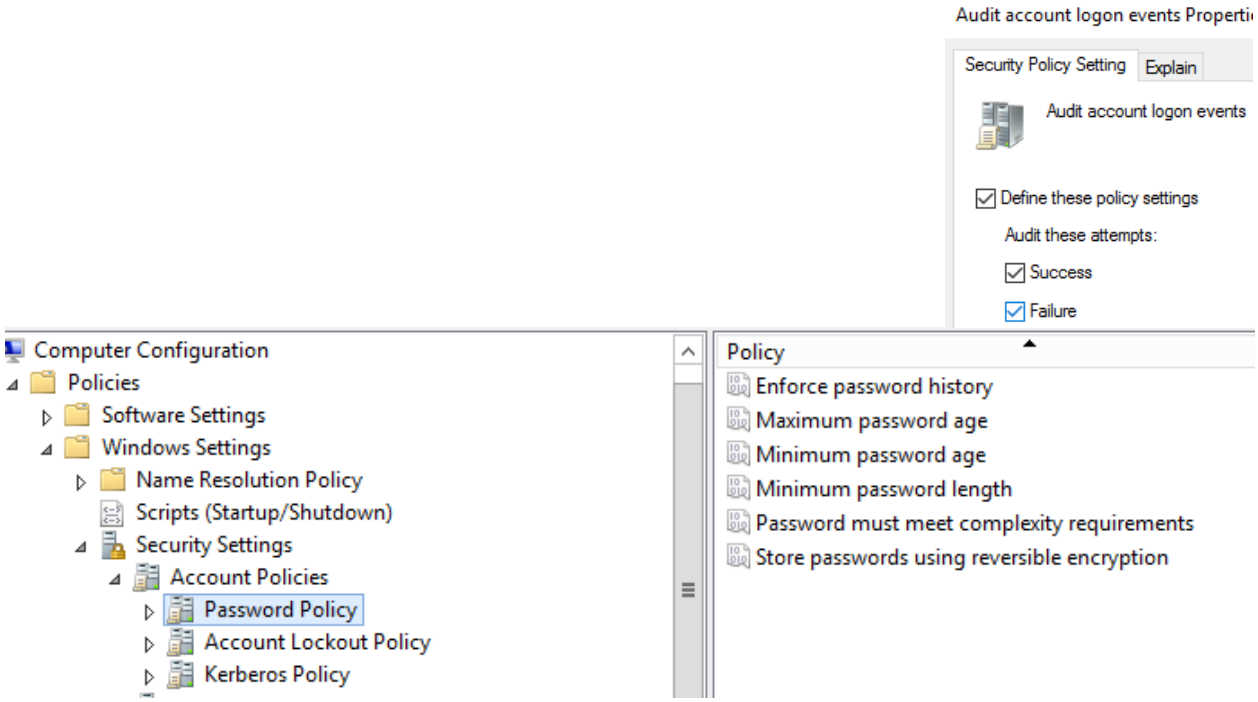
1. Set Account Password Policies:
    a. Change the minimum password length to 8 character
    b. Set maximum age to force changes every 60 days
    c. Password History change to the last 12 passwords

2. Take a screenshot of the Password Policy Settings (PrtScr #1)
3. Account Lockout Policy *(To prevent password guessing)*
    a. Lockout threshold to 5 attempts
    b. Duration for 1 hour
    c. Reset account lockout to 1 hours
    d. Lockout counter set to 1 hour, before count goes back to count of zero

4. Take a screenshot of the Account Lockout Policy Settings (PrtScr #2)
5. Kerberos Policy
    a. Verify enforce user logon restrictions is enabled

6. Take a screenshot of the Kerberos Policy Settings (PrtScr #3)
7. Local Policies:
    a. Audit Policy
        i. Enable audit of logon success and failures
    b. Security Options
        i. Interactive Logon: Prompt user 3 days prior to password expiration to change password before it expires
        ii. Shutdown: Clear virtual memory pagefile
        iii. Set Interactive Logon: Machine inactivity limit, define after 30 minutes to automatically start screensaver and lock machine

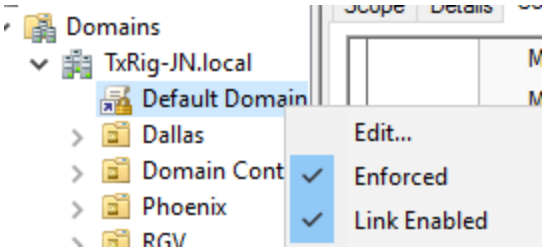
    c. Event Log
        i. Enable Event Log Retention for 14 days for Security, System, and Application logs
        ii. Take a screenshot of the Event Log Retention for Security, System, and Application logs (PrtScr#4)



8. Close Policy Management Editor

Part 3: Define and Enforce Default Domain Policies

1. Open Group Policy Management. Right click Default Domain GPO, select Edit.
2. Right click the Default Domain GPO, select Enforced and Link Enabled
3. Double click Default Domain Policy:
4. Scope Tab, verify security filtering is set to apply to all Authenticated Users, location is set to Domain Name, and enforced and linked enabled are both set to YES
5. Settings Tab: View Computer Configuration



Step 4: Test Impact Configured Domain Policies: Client must be joined to the domain

1. Logon using RGV user Edna Pena AD user account
   (Check AD Domain Users, verify the user's logon credentials, if set you can remove any time restrictions for testing, reset password if you don't recall the password, or you have problems with the password)

2. Go to the Windows Panel, in run box enter services.msc

3. Scroll down to the Group Policy client, verify this service is set Startup Type: is set to automatically.

4. To speed up GPO Client Policies push down for testing:
   Open your command line and enter the following command **gpupdate /force**
   You should see a message indicating the policy update completed successfully.

```
C:\Users\chavez>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.
```

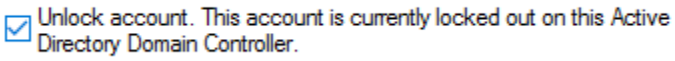
5. Logout.

6. Restart your client.

7. Test Lockout Policy by attempting to login with a valid user account but with the wrong password until you receive error message that the account has been locked out, to contact your system administrator

8. Logon with a regular domain user Edna Pena from the RGV office.
   Trigger Account Lockout by enter the wrong password multiple times.
   Take a screenshot showing the account is locked out. (PrtScr #5)

9. In ADUC on the server, view the properties of Edna Pena account, Active Directory User Account Tab. To unlock, click the box for Unlock account.



.

Reflection

1. What is the purpose of the "Minimum password age" and "Enforce password history" Group Policy settings?
2. Why should we lock the screen after a few minutes of inactivity?

Rubric

Checklist/Single Point Mastery

Concerns Working Towards Proficiency	Criteria Standards for This Competency	Accomplished Evidence of Mastering Competency
	Criteria #1: Proof Accounting Password Policy Settings (PrtScr #1) (15 points)	
	Criteria #2: Proof Lockout Policy Settings (PrtScr #2) (15 points)	
	Criteria #3: Proof of Kerberos Policy Settings (PrtScr #3) (15 points)	
	Criteria #4: Proof of Local: Audit and Security Policies (PrtScr #4) (15 points)	
	Criteria #5: Proof Client lock out – client side (PrtScr #5) (20 points)	
	Criteria #6: Answers to the Reflection questions in a text file (20 points)	