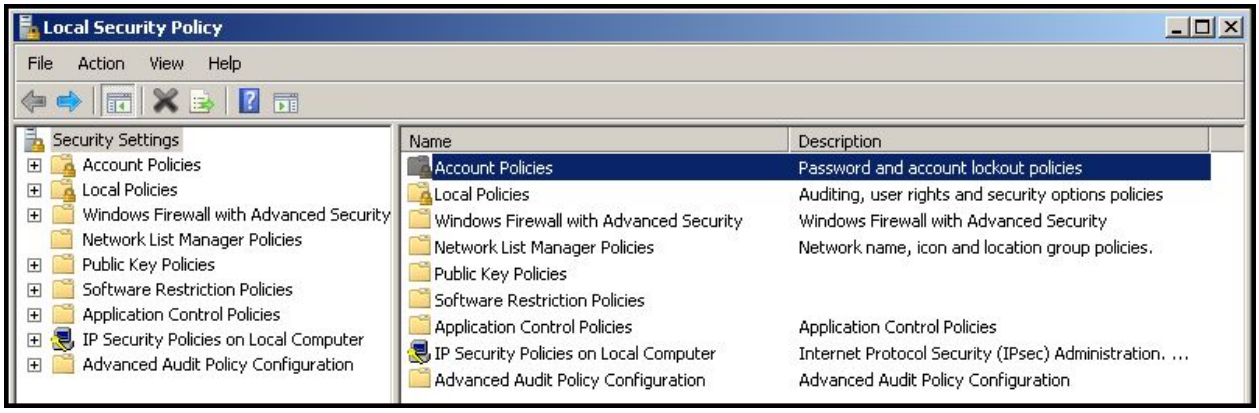
Hardening Windows 7 Using Local Security Policies

A. Account Policies

Password policy can help secure most environments through its ability to require password complexity and frequent password changes. Account Lockout policy provides the ability to automatically disable an account after a series of unsuccessful logon attempts. In this exercise, you will implement several account policies that your IT manager asks for. This activity will be performed in Windows 7 virtual machines. You can use any of them.

1. Click on **Start**, then select **Control Panel**. Click **System and Security** and then **Administrative Tools**. Double-click on **Local Security Policy** (or type **`secpol.msc`** in the Search Windows and press enter). In the window that appears, double-click **Account Policies**.



2. Implement the following policies by choosing proper Win7 account policies. For each policy request, you need to find and implement the most appropriate Windows Account Policy. In the following table, summarize which policy that you choose and implement. Please state the exact name of the policy and whether the policy is enabled or disabled.

The IT Manager's Requests	**What do you implement in the Windows 7 Account Policy?**
Users must change their password every six months.	
Passwords must be minimum of 10 characters	

Passwords must include at least one number, special character, or capital letters. All small letter passwords are not accepted.	
Users cannot use their previous password as new password when they are changing their password	
After three unsuccessful log on attempts user accounts will be locked down for 5 minutes.	

Review Questions:
Try these policies by creating a new user account. For example, try creating a user with a short-weak password. Then, try entering the password of a user three times wrong.

B. User Right Assignments and Security Options

1. Click on **Start**, then select **Control Panel**. Click **System and Security** and then **Administrative Tools**. Double-click on **Local Security Policy**. (or type **`secpol.msc`** in the Search Windows and press enter). In the window that appears, double-click **Local Policies**.
2. Implement the following policies by choosing proper Win7 account policies.

IT Manager's Requests	**What do you implement in Windows 7 Account Policy?**
Only Administrators are allowed to change system time.	
Only Administrators and Power Users are allowed to shutdown the system.	
Display "This computer can be used only by Penn State Students" for users attempting to log on.	
Prompt users 15 days before their passwords expire.	
Audit the log on to the computer.	

Review Questions:
Log on as Student2 (Password:student2) and test these policies. Include a screenshot

displaying “This computer can be used …….” in your lab report.