Advanced Security Audit Lab notes

Click Next to begin your lab exercise

1. In Server Manager, select **Tools**, **Group Policy management**
2. Expand Forest, expand Domains, expand contoso.com
3. Right-click on **Default Domain Policy** and click **Edit**
4. Select Computer Configuration, Policies, Windows Settings, Security Settings, Advanced Audit Policy Configuration
5. Expand Advanced Audit Policy Configuration
6. Expand Audit Policies
7. Select Logon/Logoff
8. Under subcategory select Audit Logon
9. Select "configure the following audit events"
10. Select Success, select failure
11. Click on Ok
12. Close Group Policy Editor box, close Group Policy Management

Ensuring that the logon policy is not overwritten by the basic logon audit policy

1. Click on **Tools**, **Group Policy Management**
2. Expand forest, expand Domains, expand contoso.com
3. Right-click on **Default Domain Policy** and select E**dit**
4. Select **Computer Configuration, Policies, Windows Settings, Security Settings, Local Polices, Security Options**
5. Select **Audit: Force Audit policy subcategory settings (Windows Vista or later) to override audit policy category settings**
6. Select **Define this policy setting,** make sure **enabled** is selected and click on **OK**
7. Close Group Policy Management Editor, close Group Policy Management
   End of Lab