Windows 2000 Hardening

Open Local Security Policy:

1. Log on to the computer with administrative rights.
2. In a Windows 2000 Professional computer, **Administrative Tools** is not displayed as a Start menu option by default. To view the **Administrative Tools** menu option in Windows 2000 Professional, click **Start**, point to **Settings**, and select **Taskbar and Start Menu**. In the **Taskbar and Start Menu Properties** window, click the **Advanced** tab. Check the **Display Administrative Tools** checkbox in the **Start Menu Settings** dialog box. Click the **OK** button to complete the setting.
3. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Local Security Policy**. This opens the Local Security Settings console.

Set password policy:

1. Open the applicable security policy through Local Security Policies
2. Expand **Security Settings**.
3. Within **Security Settings**, expand **Account Policies** to reveal the **Password**, **Account Lockout**, and **Kerberos** policies.
4. Click on the **Password Policy** object. The right-hand details pane will reveal the configurable Password Policy settings.
5. Set the Password Policy as follows:
   1. Set limit on how often password may be reused:
      1. Double click **Enforce password history**
      2. Check **Define this policy setting** box
      3. Set **passwords remembered** to 24
   2. Set max password age:
      1. Double click **Maximum password age**
      2. Check **Define this policy setting** box
      3. Set **days** to 70
   3. Set min password age:
      1. Double click **Minimum password age**
      2. Check **Define this policy setting** box
      3. Set **days** to 2
   4. Set min password length:
      1. Double click **Minimum password length**
      2. Check **Define this policy setting** box
      3. Set **characters** to 8
   5. Enable password complexity

Set local rights and privileges:

1. Expand **security settings**
2. Within **Security Settings**, expand **Local Policies** to reveal the **Audit, User Rights Assignment**, and **Security Options** policies.
3. Click on the **User Rights Assignment** object. Assign the following rights and privileges:
   1. Access this computer from the network:
      * Administrators
      * Backup Operators
      * Power Users
      * Users
      * Authenticated Users
   2. Log on Locally:
      * Administrators
      * Backup Operators
      * Power Users
   3. Shut Down the System
      * Administrators

Set security options:

1. Navigate to **Windows Settings > Security Settings > Local Policy > Security Options**
2. Set the following options:
   1. Additional Restrictions for Anonymous Connections: **No access without explicit anonymous permissions**
   2. Allow System to Be Shut Down Without Having to Log On: **Disabled**
   3. Audit Use of Backup and Restore Privilege: **Enabled**
   4. Clear Virtual Memory Pagefile When System Shuts Down: **Enabled**
   5. Digitally Sign Client Communication (Always): **Enabled**
   6. Disable CTRL-ALT-DEL Requirement for Logon: **Disabled**
   7. Do Not Display Last User Name in Logon Screen: **Enabled**
   8. Prevent Users From Installing Printer Drivers: **Enabled**
   9. Recovery Console: Allow Automatic Administrative Logon: **Disabled**
   10. Rename Administrator Account: **(Provide a good name)**
   11. Restrict CD-ROM Access to Locally Logged-On User Only: **Enabled**

Audit Log management (Up to monitoring team to determine if these changes are worth it):

1. Navigate to **Start > Programs > Administrative tools > Event viewer**
2. Right-click on **Security Log** object and click **Properties**
3. Set the following:
   * **Set Maximum Security Log Size**: 20MB
   * **Restrict Guest Access to the Application Log: Enabled**
   * **Restrict Guest Access to the Security Log: Enabled**
   * **Restrict Guest Access to the System Log: Enabled**
   * **Retention Method for Application Log: Overwrite events as needed**
   * **Retention Method for Security Log: Overwrite events as needed**

Set group memberships:

1. Navigate to **Start > Administrative tools > Active Directory and Computers**
2. Double click the domain node
3. Go to **Users** container
4. Right click the account name and select **Properties**
5. Click on **Member Of** tab and then **Set Primary Group** to edit
6. Set the following:
   * **DnsUpdateProxy** don’t edit
   * **Domain Admins** don’t edit
   * **Domain Guests** don’t edit
   * **Domain Users:** remove Guest account and disable TsInternetUser account
   * **Enterprise Admins** don’t add non-Administrative accounts
   * **Group Policy Creator Owner** don’t add non-Administrative accounts
   * **Schema Admins** don’t add non-Administrative accounts

Secure the registry:

1. Open the **Domain Security Policy** or the **Domain Controller Security Policy** as applicable.
2. Expand **Security Settings**.
3. Within **Security Settings,** right-click on **Registry**.
4. Select **Add key**.
5. From the **Select Registry Key** window, navigate to and select the desired key.
6. Click the **OK** button. A window labeled **Database Security for *path* Properties** will appear.
7. Set permissions as outlined below:
   1. \SOFTWARE\Microsoft\Windows NT\CurrentVersion:
      * **Users**: Read; This key and subkeys
      * **Power Users**: Query Value, Set Value, Create Subkey, Enumerate Subkeys, Notify, Delete, Read permissions; This key and subkeys
      * **Administrators**: Full Control; This key and subkeys
      * **SYSTEM**: Full Control; This key and subkeys
      * **CREATOR OWNER:**Full Control; Subkeys only
      * **TERMINAL SERVER USER**: Query Value, Set Value, Create Subkey, Enumerate Subkeys, Notify, Delete, Read permissions; This key and subkeys
   2. \SOFTWARE\Microsoft\Windows NT\CurrentVersion
      * **Authenticated Users**: Read; This key and subkeys
      * **Server Operators**: Query Value, Set Value, Create Subkey, Enumerate Subkeys, Notify, Delete, Read permissions; This key and subkeys
      * **Administrators**: Full Control; This key and subkeys
      * **SYSTEM**: Full Control; This key and subkeys
      * **CREATOR OWNER**: Full Control; Subkeys only
   3. \SOFTWARE\Microsoft\Windows NT\CurrentVersion
      * **Users**: Read; This key and subkeys
      * **Power Users**: Query Value, Set Value, Create Subkey, Enumerate Subkeys, Notify, Delete, Read permissions; This key and subkeys
      * **Administrators**: Full Control; This key and subkeys
      * **SYSTEM**: Full Control; This key and subkeys
      * **CREATOR OWNER**: Full Control; Subkeys only
   4. \SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
      * **Authenticated Users**: Read; This key and subkeys
      * **Server Operators**: Read; This key and subkeys
      * **Administrators**: Full Control; This key and subkeys
      * **SYSTEM**: Full Control; This key and subkeys
      * **CREATOR OWNER**: Full Control; Subkeys only
   5. \SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
      * **Users**: Read; This key and subkeys
      * **Power Users**: Read; This key and subkeys
      * **Administrators**: Full Control; This key and subkeys
      * **SYSTEM**: Full Control; This key and subkeys
      * **CREATOR OWNER**: Full Control; Subkeys only
   6. HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\ProfileList
      * **Users:**Read; This key and subkeys
      * **Power Users:**Read; This key and subkeys
      * **Administrators**: Full Control; This key and subkeys
      * **SYSTEM**: Full Control; This key and subkeys
      * **CREATOR OWNER**: Full Control; Subkeys only
   7. HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\AEDebug
      * **Users:**Read; This key and subkeys
      * **Power Users:**Read; This key and subkeys
      * **Administrators**: Full Control; This key and subkeys
      * **SYSTEM**: Full Control; This key and subkeys
      * **CREATOR OWNER**: Full Control; Subkeys only
   8. Edit the following with the same settings:
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\Accessibility
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\AsrCommands
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\Classes
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\EFS
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\IniFileMapping
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\Font Drivers
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\Windows
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\Time Zones
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\Svchost
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\SecEdit
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\Perflib
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\ProfileList
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\AEDebug
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\Accessibility
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\AsrCommands
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\Classes
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\Classes
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\EFS
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\IniFileMapping
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\FontMapper
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\Font Drivers
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\Windows
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\Time Zones
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\Svchost
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\SecEdit
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\Perflib

\*\*\*The above applies specifically to Windows 2000 but can also be used in later versions