Remove/bypass forgotten Admin Password xp/vista/win7

- Boot from a Windows boot disk and access the command prompt.
- Find the drive letter of the partition where Windows is installed, normally C: and locate the Windows folder. Eg. C:\Windows
  Note: Windows boot disks are usually given the drive letter X:
- Type the following command:
  (replace "c:" with the correct drive letter if Windows is not located on C:)
  copy c:\windows\system32\sethc.exe c:
  (This creates a copy of sethc.exe to restore later.)
- Type this command to replace sethc.exe with cmd.exe:
  copy /y c:\windows\system32\cmd.exe c:\windows\system32\sethc.exe
  Reboot your computer and start the Windows installation where you forgot the administrator password.
- After you see the logon screen, press the SHIFT key five times.
- You should see a command prompt where you can enter the following command to reset the Windows password
  net user *your_user_name aaaa*
  If you don't know your user name, just type **net user** to see the list of available user names.
- You can now log on with the password aaaa. If you wish to have no password set, now you can login, simply go to Control Panel/User Accounts and remove the password.

I recommend that you replace sethc.exe with the copy you stored in the root folder of your system drive in step 3. For this, you have to boot up again with a Windows boot disk because you can't replace system files while the Windows installation is running. Then you have to enter this command:
copy /y c:\sethc.exe c:\windows\system32\sethc.exe

DS Sept 2016