**How to “Hack” a Windows 10 Local Account**

I have used the method I am about to show you many times in helping friends and family members recover their local Windows account when they have forgotten the password. This is a simple process only requiring a few Command Prompt commands and a thumb drive with a Preinstallation Environment, for this we will be using Hiren’s BootCD.

A few important notes here is that this method can be used to reset the password of ANY local account on a Windows PC, this is including the Local Administrator account that unless has been removed by the user can be reset and logged into for complete control over the PC. There are ways to protect yourself from this attack if you are worried about it. So, enough intro, let us get to the method.

For this you will need a USB Flash drive with [Hiren’s BootCD](https://www.hirensbootcd.org/) written to it. Hiren’s BootCD is a Preinstallation environment that has a ton of useful utilities, however for this method, we will only need the Command Prompt.

Step 1:

* Insert the USB flash drive and boot to it, you should be automatically dropped into a desktop if it boots successfully.

Step 2:

Open Command Prompt and type these commands in this order: (Commands are in Red)

* 1. C: (this should change the working directory from the Preinstallation Environment to the actual hard drive of the machine)
  2. Cd C:\windows\system32\ (We want to navigate to the System32 folder of the machine)
  3. Copy sethc.exe C:\ (If you are doing this as a means to recover a lost account then you should do this step, we are copying the program that displays the sticky keys warning message after mashing the Shift Key too many times, it’s important to copy this file to the C:\ so we can reverse this process)
  4. Copy cmd.exe sethc.exe (this is overwriting the sticky keys dialog box with Command Prompt; this will be the key step in this method. If it asks if you want to overwrite the file, select Yes. And that is it for the actual “Hack”.)

Step 3:

* Reboot the machine into the Operating System and Mash the shift key until a Command Prompt window appears

Step 4:

To get a list of all the local accounts type the command net user this will display all Local accounts on the machine, you should see the persons local account if they had one, if you do you can type this command to reset their password and have them log in: net user (their username) \* it will ask you to type in a password and confirm it. If you don’t see a local username or are more interested in Admin access to the machine, you can use the same command from above but instead of their username use Administrator Windows is guaranteed to have this account however it might be in a disabled state, to fix that you just need to type this command: net user administrator /active:yes this will enable the account and you should now be able to login as the local administrator with the password you set for it.

**How to Protect against this kind of attack**

This attack has been around for a while, I first found out about it in Windows 7 where it was ridiculously easy to enter a Pre-Boot Environment. At that time, every Windows 7 machine had the ability to create a System Recovery Disk, all you needed was a CD and a machine with a CD-Drive. So you could make your own System Recovery Disk on your machine and use it on other Windows 7 machines and perform this kind of attack.

This attack is possible only if the user **does not** have Bitlocker Enabled and Active or some other kind of Preboot Protection. If the user did have Bitlocker enabled, you would not be able to access the C: until it has been unlocked with the Bitlocker Recovery Key which is a randomly generated 48-digit key. I am not sure about the Home version of Windows but the Pro version does have this feature. It can be enabled in the Control Panel and if you have linked your Microsoft Account to your PC the Recovery Key for your PC should get backed up to your Microsoft Account where if for any reason Bitlocker triggers and asks for it, you can simply login to your Microsoft Account and pull up the Recovery Key.

Personally, I have Bitlocker setup to ask for a PIN code every time I turn on my computer. In most cases I have seen where the PIN code is used at startup, if Bitlocker triggers which can happen from a Windows Update and it asks for the Recovery Key you should be able to just restart and enter the PIN code instead of the 48 digit Recovery Key. As far as I have researched deleting the Local Administrator account will not help protect against this attack as while at the Login screen if you can open the Command Prompt window it will be at the admin level so the attacker can just create their own local admin account.

So, in short to protect against this attack, simply enable Bitlocker and if you are concerned about not being able to recover a local account password after enabling Bitlocker, Windows 10 has a feature to create a Password Recover Disk. With this feature, you can type in the name of the local account and the password at the time and it will create a file that can be stored on a flash drive or cloud storage and used in the “Reset Password” options from the login screen.

I hope you found this guide helpful, if I am incorrect or there is a more efficient way of doing this task please do let me know.