**SOP OF WINDOWS PASSWORD HACKING**

**METHOD 1: USING HIREN BOOT CD RESET WINDOWS 10 PASSWORD AND BYPASS THE AUTHENTICATION**

**Step1**: Download Hiren’s Boot CD (older Version: <https://www.hirensbootcd.org/old-versions/>)

Graphical user interface, text, application

Description automatically generated

**Step2:** Make a bootable pen-drive (If you want to test this method on real machines and not virtual):

**Step2a**: Download Rufus. (<https://rufus.ie/en_US/>)

A picture containing background pattern

Description automatically generated

**Step 2b**: Attach a pen-drive to your system. (Minimum: 8 GB)

Graphical user interface, text, application, email

Description automatically generated

**Step 2c**: Select the Hiren's.BootCD.15.2 .iso file:

Graphical user interface, text, application, email

Description automatically generated

**Step 2d**: After selecting the iso file click on START.

**Step 2e**: After the status is ready click on CLOSE.

Graphical user interface, text, application, email

Description automatically generated

**Step 3**: To test this method, make sure your Windows 10 requires you to enter a password to enter the system.A picture containing text, nature, outdoor

Description automatically generated

**Step 4**: Now attach your bootable pen-drive to the system before starting the system else If you want to test this method on Virtual machines do the following:

**Step 4a**: Open the Virtual Box and Select the windows machine, go to SETTINGS>STORAGE.

Graphical user interface, text, application

Description automatically generated

**Step 4b**: Now add an optical drive (Hiren's.BootCD.15.2 .iso file) by clicking on the icon on the left.

Graphical user interface, text, application

Description automatically generated

**Step 5**: Now Start the Windows Machine.

**Step 6**: When you see the Virtual Machine Logo press F12, you will see the below screen.

Text

Description automatically generated

**Step 7**: Now press c (which is for CD-ROM) on the keyboard to get prompted to the Hiren’s Boot Menu.

Text

Description automatically generated

From the Hiren’s Boot Menu select **Offline NT/2000/XP/Vista/7 Password Changer** and press ENTER.

Text

Description automatically generated

**Step 8**: You will get the following screen (Boot prompt). Press ENTER.

Text

Description automatically generated

**Step9:** The screen will list all your partitions and you need to select the partition where Windows is installed. In most of the cases you will see that 1) is the small 500Mb boot partition and 2) is the larger Windows partition. In my screenshot you can see that I got only one option so I will select that. So, I type **1** and then press ENTER.

Text

Description automatically generated**Step 10**: Now it will ask to confirm the registry path (Windows/System32/config). The default registry path will be correct so just press ENTER.Text

Description automatically generated

**Step 11**: After you press Enter you will get the following screen:

Text

Description automatically generated

**Step 12**: Now our task was to reset the password so we will type 1 and ENTER. After doing so we will get the following screen:

Text

Description automatically generated

**Step 13**: Now we want to edit user data and password so we will type **1,** and press ENTER. After doing so you will get a screen which will show you the usernames and their details.

(My username is IEUSER)

Text

Description automatically generated

**Step 14**: You know the username for which you want to reset the password so type that and press ENTER.

Text

Description automatically generated

**Step 15**: Now you will get the following screen. To clear the password type **1** and press ENTER.

A picture containing text, screenshot, battery

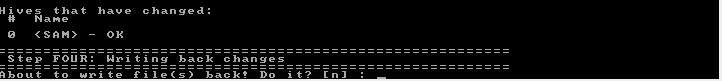
Description automatically generated

**Step 16**: After this you will get the “Password Cleared!” message. Now you can quit by typing **!**.

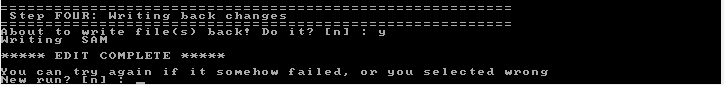
Text

Description automatically generated

**Step 17**: Now type **q** and press ENTER.



**Step 18**: To save the changes type **y** and press ENTER. It will show “EDIT COMPLETE”



**Step 19**: You will get the following screen, type **n** and then press ENTER.

Press CTRL-ALT-DEL to reboot.

A picture containing text

Description automatically generated

**Step 20**: Now when you will start you Windows 10 machine again you will see that you no longer need to enter the password to enter the system.

A picture containing nature, arch

Description automatically generated