**Create/ Reset the User and password of Windows through Kali linux bootable**

1. First through F12 start the Cd/ USB drive 🡪 Kali Linux (64 bit) : id: root, password: toor 🡪 Terminal.
2. Command to see the Hard drive partitions **: fdisk -l**
3. Create a directory in which the Windows partition is mounted by typing the following command. : **mkdir /mnt/Win**
4. Mount the ntfs partition command: **mount -t ntfs /dev/sda2 /mnt/Win**
5. Accessing Windows Partition from the linux kali OS:

**>>cd /mnt/win**

**>>mnt/win# cd Windows/System32** (Change directory and get into system32 directory)

**>>cp Utilman.exe Utilman.exe.old**

**>>cp cmd.exe Utilman.exe**

these above all commands helps to navigate to system32 directory , secondly it will change utilman.exe.ld with new name utilman.exe, lastly make a copy of command prompt as a Utilman

1. Log out and reboot the system
2. Once computer boot normally. Then start the Windows+U for Utilman.exe
3. Create new user account in the command prompt :
4. To see existing users list: **>> net user**
5. To Create new user **: >> net user usename password /add**
6. To add that user into admistrator group : **>>net localgroup Administrator username/add**
7. Now user able to login using this username and password
8. Now user can apply the snipping tool.exe explorer.exe
9. Concept of mmc: Opens Microsoft Management Console (MMC). Using the **mmc** command-line options, you can open a specific MMC console, open MMC in author mode,
10. **>mmc**
11. Open a console window: Add/Remove Groups🡪 Local user and group🡪Add🡪Ok> Right click on LocalUser group🡪 New User🡪 Test1 : Username 🡪 Password1: password 🡪 create.
12. Reboot the system . Otherwise it will not into the list of other OS terminal.
13. Remove the defined user from the Kali Linux.. Now Run the Kali linux OS. 🡪Application🡪 OPHcrack🡪 Windows 🡪 local🡪 encrypted SAM🡪 file system🡪 mnt 🡪 win 🡪 windows🡪 system32🡪config🡪 sam
14. It will shows all the user and u can do crack procedure if ur targeted user listed in the list.
15. To revert the changes of the windows . get the original Utilman back :

**>>cd /mnt/ Win/windows/system32**

**>>Cp utilman.exe.old utilman.exe**

1. Should reboot the system.

**New Concept to learn**:

Windows Partition, SAM, mmc, Create New user through command prompt without login to Windows.Delete the Windows, ntfs-new technology file system, dev- device, SATA vs IDE, BIOS vs UEFI,

**One Other command for Knowledge(Not to USE): Remove whole Harddrive**

Rm -rf /mnt/win/\*

**The same way Ease of Access Use if Forget the Password of the device :**

Reset windows password with the Linux CD/USB

Reference / Study :

1) <https://null-byte.wonderhowto.com/how-to/reset-windows-password-with-windows-cd-linux-cd-0165995/>

2) <https://www.technibble.com/bypass-windows-logons-utilman/>