

# Forum:[Hack Forums](#)

Thread: [Bypass Windows Password \(Offline Hacking\)](#)

Vayxa - April 30, 2017, 3:36 am

Hello all, i'm vayxa and here the tutorial (i am not good at english sorry if i use wrong grammar)

Item needed:

1. A computer running windows os (victim)
2. Flashdisk (if you have the 16 gb its good)
3. Internet (for download iso)
4. A luck (hope the victim doesnt comeback when you by pass their login screen)
5. Rufus app

1. Download rufus
2. Download ubuntu or kali linux
3. Get yourself a flashdisk (8 gb is recommended)
4. Burn your ubuntu or kali linux iso to your flashdisk using rufus
5. When its done eject your flashdisk
6. Put your flashdisk to victim computer
7. Turn on the computer
8. Go to bios setting as soon as possible (in most case press esc or f8)
9. Choose your flashdisk in menu
10. Just wait until your ubuntu or kali boot is done
11. Open file and select disk (if your victim shutdown the computer in right way it should okay but in some case you can not open the disk, i already tried it with kali linux and its work)
12. Choose disk that contain windows (C: is default)
13. You maybe already know the next step. But if not here:
  - go to c:\windows\system32\
  - search sethc.exe rename it to sethc.exe.bac
  - search for cmd.exe and rename it to sethc.exe
14. Power off the computer
15. Turn on again

16. Press shift key repeatedly until you see cmd in screen

17. Input this command

- this will add user named pentest as admin

Net user pentest /add

Press enter

net localgroup administrators pentest /add

Press enter

Shutdown -r -t 00

Press enter

When you already restart the computer just click the new administrator user that you have been created, yeah its pentest and hoala you already get access to victim computer

18. Here my result when i test this to my own computer (using kali linux)

I can't open the disk but when i shutdown the computer completely and unplug the cable from electric socket and tried it again. I can access the disk

In theory you can copy victim files to your flashdisk (you can access their disk remember?)

So its all

Thank you.

?

**Mr. Kim** - April 30, 2017, 6:52 am

Useful tut for those who don't know about the many holes in the windows login system. Cheers :)

**Huzo** - April 30, 2017, 10:09 am

Thanks for the tutorial mate. Cheers!

**oRequiem** - April 30, 2017, 5:47 pm

You can just make a new user, make that Administrator permissions and you can change the password in your window options somewhere in the Control Panel lol.

**Faith Connors** - April 30, 2017, 5:51 pm

Or just write a chntpw liveUSB and turn 20 steps into 3.

**Zenomhunter** - April 30, 2017, 5:52 pm

If his is on windows 7, the alt is forcefully turn off the comp during startup and when you turn it on, there Will be a prompt which asked you would you like to repair your computer and you click yes and then I'll come back with them is that there were no issues detected and then it'll show you a text pad and you open that and then you go to file then open and then you can actually edit and change the sethc and The CMD the same way...just easier in my mind

**Xphile** - April 30, 2017, 6:00 pm

Nice tutorial man, thanks a lot for sharing. ?

**MarkDice** - April 30, 2017, 6:05 pm

Didn't know it'd be this easy, gotta say thanks for sharing!