

Forum:[Hack Forums](#)

Thread: [\[Tutorial\] How to Bypass Windows Password \[7, Vista, 8, 8.1\]](#)

Isildur - May 17, 2014, 11:17 am

Bypassing Windows Admin Login

This tutorial is based on the fact, that sticky keys are triggered even at Windows Login screen. Taking advantage of this, we will actually change our sticky keys app to command prompt and reset the password.

Requirements Basic knowledge of computer

Windows Disk (Should be bootable)

A Windows Operating System

Let's begin Insert your Disk in your drive.

Restart your computer

At the stage when you are asked "Press any key to boot from CD....", just press a key to step into windows setup.

Once there, click the option of Repair Computer.

Now, windows is gonna search for problems, so you are gonna wait.

Now you will be given a wizard, which in the first step asks you to select the Windows OS dir. Click the appropriate one, then click Next.

Now it may present you the option of "System Restore", just decline it, click Next.

Now startup Repair will report that it has failed & shit.

It will tell you "Can't repair your windows... " Just click Don't Send.

Now you will be in the final step of the wizard, you need to click this link at this point that says "View advanced options for system recovery and support"

This will take to a new window, there you must click on "Command Prompt" or "Cmd"

Wow! You have completed half the work!

Now, get a glass of water or just give yourself some rest. Since in the next step, you are gonna type in some big commands in the CMD window.

The Replacement of StickyKeys App First we make a copy of original Sticky Keys Code copy

c:\windows\system32\sethc.exe c:\

Now we over write the sticky keys App with command prompt, using: Code copy

c:\windows\system32\cmd.exe c:\windows\system32\sethc.exe

Final Step: Gaining your PC back!

Reboot your PC now.

When at the Login screen, press SHIFT 5 times to trigger sticky keys. (If you have disabled sticky keys, google for more sticky key commands, there are many.)

Now it will bring the command prompt window.

Type in this: Code net user Isildur PASSWORD!

Now your new password is: PASSWORD!

Voila! Done!

Placing Sticky Keys App back

Well we copied your app in C:/ (named: sethc.exe). Just copy it back to system 32 and you are done!

Any problems post here....

~ Isildur

Polymath 1.0 - May 17, 2014, 5:05 pm

While I applaud your desire to be helpful, this is the Windows Sticky Keys Exploit and has been known for a decade and a half when MS instituted the Ease of Access provision for XP/Vista/7/8. The web and this forum is littered with thousands of tutorials detailing this. BTW on XP/Vista/7/8 you need only press Shift+ F10 at the first GUI dialogue screen when booting from the Windows installer media to get a command prompt. You don't need to have the Recovery/Repair Console open or go through the steps you outline to get a command prompt. After one is finished with the command line constructs and exits the command processor, pressing Esc will terminate the installer without actually installing anything to the existing O/S.

Take care

archangel.dmitry - May 17, 2014, 10:05 pm

Obviously useless if hard drive is encrypted which it should be. Thanks for trying though.

Isildur - May 18, 2014, 2:58 am

(May 17, 2014 10:05 PM)archangel.dmitry Wrote: [\[CITE\]](#) Obviously useless if hard drive is encrypted which it should be. Thanks for trying though.

Ah, welcome. ?

I will update the tut soon with pics.

al_gharib - May 18, 2014, 10:07 am

Thanks a lot for your tuto really nice

Isildur - May 19, 2014, 12:01 am

(May 18, 2014 10:07 AM)al_gharib Wrote: [\[CITE\]](#) Thanks a lot for your tuto really nice
Oh great that you like it :)

?

Thank you!

ëdoz? - May 19, 2014, 3:07 am

Great tut, gonna play around with it haha
cheers!

Isildur - May 19, 2014, 3:35 am

(May 19, 2014 03:07 AM)ëdoz? Wrote: [\[CITE\]](#) Great tut, gonna play around with it haha
cheers!

Glad to hear that you like it

[img]<http://x.hackforums.net/images/smilies/blackhat.gif>[img]