Windows login screen bypass

LTAT.06.002 Andmeturve

Author: Mihhail Plohhotnitsenko
Supervisor: Meelis Roos

Tartu 2019
Introduction

Windows login screen bypass is a known vulnerability taking place in all windows operating systems starting from windows 95. Basically what it does is that it allows user to login into secured with password windows account without actually knowing the password. There are a few different scenarios approaching that on different versions of windows, some of which i will cover here, showing how they work and how to protect your computer against them.

Vulnerability Description

The main target of that exploit is to get access to the **command prompt** *(windows operating system console)*, where after some manipulations you will be able to reset any local account’s password and login. Obviously you will need a physical access whether to computer or it’s hard drive, where the operating system is installed to. Vulnerability lies in things we are able to do before logging into the account, such as using **ease of access** *(windows component, containing assistive technologies)*, triggering the **sticky keys** *(functionality, which allows to remain active windows modifier keys till other key is pressed)*, accessing the **Boot menu** *(special user interface used for computer pre-boot configurations)* or **advanced boot options menu** *(windows’s special startup menu, which provides some advanced functionalities)*.

Accessing the boot menu or advanced boot options will provide you to perform actions, such as booting from other drives, including USB-drives or resetting the system to factory settings, which is not our goal, but it’s very harmful also, in some cases it provides straight access to the command prompt, where we can reset the password, if it does not, we can still access it through booting from flash-drive with windows operating system installer on it, after what we should modify some files in our original drive’s system32 folder, which can be **sethc.exe** or **Utilman.exe** which corresponds to sticky keys and ease of access functionality. After some manipulations with them, we will have opportunity to run command prompt from the windows login screen, which easily allows us to reset password for any local account, in case there are no local accounts, but only microsoft ones, you can whether enable build-in administrator account or create a new one.
Exploit

Basically, all we need to do is to rename them to whatever name, copy file named cmd.exe, which is used to run command prompt, paste in same

1. **Advanced Boot options**

   To enter that menu:
   - on Windows 7 press **F8** on computer boot up, after what select “Repair Your Computer” option
   - on Windows 8-10 hold **SHIFT** and press restart button

   After that you will see that menu (if it is not disabled):

   On Windows 8-10

   ![Choose an option](image)

   Select “Troubleshoot”

   ![Advanced options](image)
On Windows 7

After what you want to select “Command Prompt” option, which will open console if it is not protected.
If that succeeded, proceed to the “End Steps”

2. **Boot from flash drive**

   For this one you will need a flash drive with any windows installer that you can boot from.

   - Insert your flash drive in your computer.
   - Enter boot menu, by pressing one of those keys **ESC, DELETE, F1, F2, F3, F11** or **F12**, usually it is written somewhere on boot up, which key enters BIOS and Boot menu.
● Then you select your USB device and boot from it
● Click "Next" on language selection

● Click “Repair your computer” option
● You will enter advanced options menu, where you need to select “Troubleshoot” option, after what proceed to “System Image Recovery” and choose your operating system.

![Advanced options](image1.png)

● On warning pop up click “cancel” and click “Next” on menu

![Warning pop up](image2.png)

● On warning pop up click “cancel” and click “Next” on menu
• By next click on “Advanced” and select “Install a driver” option after what click “Ok”
• Explorer window will open, where you will have to go to your system32 folder on your original drive with windows account (“Your Drive”>Windows>System32)
• Now you can choose whether to manipulate with ease of access or sticky keys file, navigate one of them, rename to whatever you want
• Navigate to cmd.exe file, copy it and paste in the same folder and name it after previously selected file, so in case sethc.exe name it “sethc.exe”
• After that is done you can click cancel, exit to the advanced options menu and select “Continue”, you will boot in your original windows
• After you got to the login screen there are two possibilities:
  o If you were manipulating with “sethc.exe”, then press five times on SHIFT key
  o If you were manipulating with “utilman.exe”, then press ease of access button

![Ease of Access Button](image)

• And the command prompt will appear, now you can proceed to the “End Steps” section
END STEPS

● After you got to the command prompt, type “net users” to check what accounts exist there and select the one you want to break in
● Type “net user <account name> *” and you will be asked to enter the new password for that account, enter nothing or whatever you want
● Type “exit” to exit the command prompt and now you can login to your account with the password you just set

IF you were not able to do that, cause your account is authorized with microsoft, then you will not be able to login into it, however you can create another account to at least login into that computer, after what you can copy/get all you wanted from other accounts. In that case follow next instructions:

● Create new account by typing “net user <username> /add”
● Add newly created account to administrators group with command “net localgroup administrators <username> /add”
● Type “exit” and login into it

And that is it you are in the computer with all privileges/files/information.
1. **Advanced Boot options**

To prevent other users from entering advanced boot options menu proceed to do following:

- Open command prompt with administrator rights (In windows search function search for “cmd”, right click on it and select “run as administrator”)
- Type “Reagentc /disable”, that will do it

2. **Protect Boot menu**

Not all but some computers will prevent booting from other drives if BIOS is secured with a password, that is what you should do also, because BIOS provides access to boot menu also.

So:

- Enter BIOS menu by pressing one of those keys **ESC, DELETE, F1, F2, F3, F11 or F12**, usually it is written somewhere on boot up, which key enters BIOS and Boot menu.
- Go to “Security” tab

- Select Set Supervisor Password

- Set up a password for entering BIOS menu
3. **Disable “sticky keys”**
   - Open control panel by searching for it in windows search
   - Select “Ease of Access” option
   - Press on “Make the keyboard easier to use” link
   - And there toggle off “Turn on Sticky keys” if it is on and go press on “Set up Sticky keys” below also and turn off option “Turn on Sticky Keys when the SHIFT is pressed five times” there as well

4. **Disable “ease of access”**
   - Enter command prompt with administrator rights
   - type: "\reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Utilman.exe" /v "Debugger" /t REG_SZ /d "systray.exe" /f"

   This will make ease of access button useless

5. **Protect your hard drive**
   In addition you should concern about protect whole your hard drive by encrypting it, so no one could steal anything from it and windows build-in EFS encryption is one of good choices for that, thus it protects files according to the user password, so if the password will get removed all the files will be unreadable because of the EFS encryption
   So to do that:
   - Navigate to folder or file that you want to protect with EFS
   - Right click on it and select “Properties”
   - Click on “Advanced” in general tab
   - Tick the **Encrypt contents to secure data** and you are done

   Now anyone who got to break your password and logged into your account could not read those files.
References

1. https://www.youtube.com/watch?v=RCInsJ6BLiY
2. https://www.youtube.com/watch?v=LEFV3bc0q7E
4. https://www.youtube.com/watch?v=aeWySqwqEvw
7. https://www.youtube.com/watch?v=XwUQJURKWyg
8. https://www.lifewire.com/how-to-reset-a-windows-8-password-2626230
10. https://www.youtube.com/watch?v=3-LHJ3l_xPA
11. https://superuser.com/questions/196989/how-to-remove-or-disable-ease-of-access-button-on-windows-7-login-screen