

Forum:[Hack Forums](#)

Thread: [\[TuT\]Hack admin password from guest account](#)

Ruyuk - January 9, 2011, 7:13 am

Ever wanted to hack your college PC with guest account/student or just wanted to hack your friend's PC to make him gawk when you tell him 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 system32.

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. 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 ARMAAN/ADD" where "ARMAAN" is the username you would like to add with administrator privileges. Then hide your newly created admin account by -

Go to registry editor and navigating 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 you created for your admin account! ???

Ruyuk - January 10, 2011, 9:56 pm

No one found this TuT useful?

the_lol - January 10, 2011, 10:08 pm

So for this to work.. you need to already have access to the "admin" account on the computer. Nice tutorial.. nice concept but pretty useless. Thanks for the share though<3.

Ruyuk - January 10, 2011, 10:10 pm

(Jan 10, 2011 11:08 PM)the_lol Wrote: [\[CITE\]](#) So for this to work.. you need to already have access to the "admin" account on the computer. Nice tutorial.. nice concept but pretty useless. Thanks for the share though<3.

No, why would you need Admin access in the first place? What would be the point of this lol?

the_lol - January 10, 2011, 10:35 pm

Oh nevermind. I didn't understand it at first. Good guide actually. Extremely unique. <3

duexx - January 10, 2011, 11:19 pm

i will prolly, try it out later ;)

Thank you for the tutorial

Compax - January 11, 2011, 12:20 am

will see if this works later on ;)

Thanks for the tut ;)

WinnieThePooh - January 11, 2011, 12:25 am

My friends say it works. I'll try this later.

- Thanks mate.

twain - January 11, 2011, 12:42 am

i've never thought about hacking with sethc.exe, that's pretty cool xD
nice work, thanks dude

Reported - January 11, 2011, 12:50 am

Awesome guide dude, Never saw anything like this before.

I am going to test this now ?

Ruyuk - January 13, 2011, 5:08 am

You are all welcome, I hope this helps you especially when you forget your Admin password :)

princeofindia - January 13, 2011, 5:38 am

Nice tut... Will try it someday if needed... :P

sonu000a - January 14, 2011, 9:17 am

not this is not work when i am trying to replace sethc.exe it says "access is denied make sure your disk is write protected".

teclas - January 17, 2011, 2:18 pm

Oh, great! Thanks! Going to try it out.

T@M3R - January 17, 2011, 4:42 pm

it is a new thing, never heard of it before.
im gonna try it in our school and report back asap

thnx

spyke8x - January 17, 2011, 4:46 pm

Very nice, but the system administrator has to be retarded to allow guest to have write access to any system directories.

dstn1211 - January 17, 2011, 4:50 pm

(Jan 17, 2011 05:46 PM)spyke8x Wrote: [\[CITE\]](#) Very nice, but the system administrator has to be retarded to allow guest to have write access to any system directories.

If they haven't blocked booting off of discs or USB flash drives, there are always live operating systems... ?

Tw15t3d - January 17, 2011, 9:36 pm

Thank you Ruyuk, this tutorial was VERY helpful :) I highly appreciated it

Ruyuk - January 18, 2011, 2:28 am

You guys are all welcome. :)

Ruyuk - March 8, 2011, 7:13 am

This should be useful to some more of you guys....

PhineasPhreak - March 8, 2011, 8:57 am

Found it useful but seriously which guest account actually has system32 privileges.

It seems that I keep hating on your threads... I'm sorry.

Hano - March 8, 2011, 9:00 am

I can't access System32 folder.... I'm only a guest member.

sid8012 - March 8, 2011, 9:00 am

It only works if your school or network has no security, which is unlikely unless your school is shitty.

snake_escape - March 9, 2011, 2:45 pm

Make a shortcut to C:\ and that will usually work. Otherwise your screwed...

Ruyuk - March 9, 2011, 8:19 pm

Guys, don't forget to rate this thread please! Thank you.

Joey Tribbiani - March 10, 2011, 12:11 am

5 stared :)

Nice tut ! You deserve it :D

IFingerUrMum - March 10, 2011, 4:06 am

you need admin rights to copy cmd to desktop,

on vista

gg

m_DarkLord - March 24, 2011, 12:53 am

Thanks for the tut very helpful.

Vertu - March 24, 2011, 12:54 am

Very good way way to hack ,like this. Very simple but usable!

Cunicul - April 12, 2011, 11:09 am

Thanks a lot for this as well! :D

GooseMonger - April 12, 2011, 3:55 pm

Hmm... I need administrator privileges on Windows 7 in order to be able to write into system32. But maybe one of my LiveCDs for a Linux will do it. I hope so, because this is just what I needed to do...

On a side note, would it be perhaps possible for a batch file to do this, if ran on an administrator account? I expect it would, but I'm unsure if I know how to rename the cmd.exe into the needed name.

thehardway - April 12, 2011, 4:36 pm

thankss, pretty helpful..

The Free Crypter - April 12, 2011, 5:13 pm

Nice tut, IM using this Tomorrow For Sure Dude :D

GooseMonger - April 12, 2011, 6:38 pm

Well I finally got around to doing it, and I must say... so long as the person doing this uses a little free-thinking about how to copy something into the right location even if it's supposed to be blocked, this is an exceptional tutorial, and the thought behind it is just brilliant.

Thank you very much, it worked flawlessly.

if I could, I'd be giving you rep for this, but sadly I can't do such a thing.

Grey-Tech - April 12, 2011, 6:51 pm

Hah! That's just brilliant! A very nice share, I'm gonna remember that one and try it out in the future. ;)

ITz Kr4k 4 J4Ck - April 12, 2011, 7:01 pm

Thanks this is awesome il try it soon:)

zrokwl - April 12, 2011, 8:13 pm

Funnily enough was looking for a tut on this tonight cheers man :D

temaki - April 12, 2011, 9:19 pm

Is there a way to enable write access from a guest account? o.O

?ringles - April 12, 2011, 9:38 pm

nice man will try this out!

RoLLs Ro?CE - April 12, 2011, 9:57 pm

The thing is my school computers got some novel shit installed on it and u cant go in the C drive, but would it still work if u do the notepad batch method how u save it as .bat at the end.?

T0x1c - April 12, 2011, 10:08 pm

Great tut. Never thought of using sticky keys as a vuln. This is a great idea and i will try it later. ?

hermiod - April 13, 2011, 12:02 am

Nice tutorial.. nice conecept . Thanks for the share though<3.

hacKBoTneT - May 22, 2011, 2:36 am

Great.. Thanx for the share... Continue posting like this..

D3x73r - May 22, 2011, 3:00 am

Ooo nice :) I like it :D

gamer11fw - May 22, 2011, 3:06 am

This has been posted somewhere else but without the guest account, they used a livecd. But cool to write this thx! and btw do you know if it works on windows 7 to rewrite a file in system32? (no need admin privileges)?

sexy-intruder - May 22, 2011, 3:12 am

thanks nice share i will try

Ankush - May 22, 2011, 4:29 am

very very old method and not useful at all..

Mr.Steven - May 22, 2011, 4:41 am

Oh mate.Nice & unique trick,liked that!

Nice share!

Chzn4lifez - May 22, 2011, 6:28 am

Very nice find but what Windows OS does this work for?

RussianFederation - May 22, 2011, 6:33 am

Great tutorial bro. ?

Daffodil - May 22, 2011, 8:34 am

Need to check....

thnx anyway.

?r1PP|? - May 22, 2011, 9:46 am

Nice tutorial, I'll try it tommorow :)

Baconator - May 22, 2011, 10:36 am

This looks very detailed and complete, I'll try it sometime.

phybe? - May 22, 2011, 10:37 am

This is quite an interesting method I have not seen before, thanks for the great tutorial!

princedynamite - May 23, 2011, 12:44 am

very usefull TuT! thnQ very very much!

Mr.Feelgood - May 23, 2011, 1:02 am

Will try it out, looks great:D THX! But... im just gettign finished with shcool, and we get computers next year lol, so no hackign on my shcool comps:((

kyur3k0 - June 26, 2011, 4:42 pm

Has a flaw to it, though.

On Windows 7, you cannot edit/delete/move anything to the Windows folder. Needs Admin priv.

Just tested; didn't work. Might test it on Windows XP sometime. Nice thinking, nonetheless.

-k

Krawk - June 26, 2011, 7:31 pm

Nice guide bro will be helpful to me

Saintzfan - June 26, 2011, 7:47 pm

Wow, thanks. I can use this.

apt-get money - June 26, 2011, 8:30 pm

im going to london in 30 minutes.

this shit is so fucking good i will think about it every day i will be there ,

and trying this tutorial will be the first thing ill do when i come home.

thanks alot , HQ mf -squawck- n sh -squawck- t .

Yellow™ - June 26, 2011, 8:43 pm

Yes, very very nice guide. I have never knew about anything like this. ^ _ ^

Chutiya hun mien - June 26, 2011, 9:18 pm

Amazing. I will do this for my friend now as his brother has given him the guest account and no admin privileges

Infidel - June 26, 2011, 10:01 pm

I would think you need to have admin to replace a file in sys32

thehackerboy - June 27, 2011, 8:03 pm

this is a great tut for scholars like me . i will hack my principal account with this haha.

??LI?? - June 27, 2011, 9:34 pm

Lol I guess i'll try this when i go to my friends or something.

nnkvnus - June 27, 2011, 10:09 pm

Nice tut...

I just want to put this out there, on some computer you can right click "my computer" go to "manage" on the guest account and then user group then right click on admin user and click reset pass word. this trick does not work on factory install or professionally installed os. Also i have been told when you reset password in these manners, it will destroy any encrypted file made by the os, so beware. you can fuck some one up real good when you reset his password.

^ Slaughterer ^! - June 27, 2011, 11:10 pm

Ahh, wanted this and got it! Thanks for sharing

TimeGhost - June 28, 2011, 2:00 am

This is very cool for sure! Definitely going to try it out! Thanks!

[[R9]] - June 28, 2011, 2:03 am

Seems cool to me man op though i knew this already.

Mr.Steven - June 28, 2011, 2:04 am

Really nice guide but I think that guest can't copy/rename files from/to system32.

bwood74 - June 28, 2011, 5:13 am

Good TuT...to bad I can't access C drive on school computers -.-

Zeus1887 - June 28, 2011, 5:39 am

Yea i have similar thread like this but simpler but thanks anyway !

~Råwr~ - June 28, 2011, 5:44 am

nice tut man its really goood

Great Prosperity - June 28, 2011, 1:10 pm

This should be helpful whenever my dad has forgot to give my brother the password xD

QBUGS - June 28, 2011, 4:41 pm

I thought you need admin priveleges to rename something in system32?

Nice tut ;)

xVWhiteboy - June 28, 2011, 4:47 pm

Good tutorial, noob friendly, will surely help someone.

Valour - June 28, 2011, 6:46 pm

Share was very good but this is posted a few times in different sections. I remember that i know this method since the last year and I had read it somewhere on HF itself. But still thanks for bringing it back.

Kill?Muvz - June 29, 2011, 6:24 am

(Jan 10, 2011 11:10 PM)Ruyuk Wrote: [\[CITE\]](#) No, why would you need Admin access int he first place? What would be the point of this lol?

Because most guest accounts don't have enough previledged to move/rename/delete files in the system folder.

(Jan 10, 2011 11:10 PM)Ruyuk Wrote: [\[CITE\]](#) No, why would you need Admin access int he first place? What would be the point of this lol?

Because most guest accounts don't have enough previledged to move/rename/delete files in the system folder.

FastFive - June 29, 2011, 6:32 am

seen this before a couple of places but whatever

!ron m@n - June 29, 2011, 6:45 am

Nice Tut bro =] Keep it up!

slimshadylover - June 29, 2011, 5:26 pm

Although this is a nice tutorial, guest accounts usually do not have the privelege of writing/deleting/modifying items in the system32 folder, any ideas?..

Slim

h4kr! - June 29, 2011, 6:20 pm

sometimes a pc will have an acount(or 2!!)in the admin group(says their "system administrator") but i think thereis somethin those acc cannot do.(also,when "running as..."there's someone named "Adminitrator."[xp]if you select it says incorrect password)
those accounts may change users,etc. but not run the program :\nwhen i do this i might change the password.LOL

Loefah - June 29, 2011, 6:22 pm

Awsome guide worked like a charm thank you :)

BestRacs - June 29, 2011, 7:17 pm

Very good tut. Keep up the good work.

I see allot of parrots here hehehehehe

I scrolled true the whole thread and see the same answer over and over again.

Instead of repeating the person above you just say thanks or nothing ;).

Its very annoying to scroll true a thread looking for additional info if everybody is repeating each other.

Thanks again bro.

Infobesity - June 29, 2011, 7:50 pm

Similar to the screen saver method.

krishnav891 - June 30, 2011, 11:30 pm

nice it work thanks for the post keep going :D

??????™ - June 30, 2011, 11:40 pm

Looks good i will try it to check if it works.

?Sean - June 30, 2011, 11:42 pm

Nice tut bro! Helpful :) Thanks for this

zzyx - July 1, 2011, 2:59 am

nice, this doesn't take much time and it is very good!

neat dice - July 1, 2011, 3:12 am

lol ;o this is great!!@!@@!@!@!

lol ;o this is great!!@!@@!@!@!

FusionGT - July 1, 2011, 4:04 am

Thank you, this really helped me.

godsp33d - July 1, 2011, 4:07 pm

Now this is what I call thinking creatively!

coldfiret - July 6, 2011, 11:38 pm

Another great guide by Ruyuk, I used this to hack school comp.

KnuttyD - July 6, 2011, 11:45 pm

So you dont need admin to write to the system32 folder?

Whatisthismadness

Death by Stereo - July 6, 2011, 11:56 pm

But the problem is, any guest account will not have access to editing files like that.

Sky God - July 7, 2011, 2:08 am

I'll try this out next time I go to my friends house. He's all dodgy about his shit and this will be perfect to freak him out.

ethico - July 7, 2011, 3:20 am

not useful for windows 7 worked well in case of xp and vista...

Frequenceh - July 7, 2011, 3:31 am

This is very smart

lol i thought you could only hack with the safe mode thing.

good thinking ;)

agentblackhole - July 7, 2011, 6:36 am

Most likely you will not have access to the Sys32 folder, however sometimes clearing a admin password to log into the machine isn't plausible, so deleting the hash wont work well... and the password is random enough or long enough not to exist in standard rainbow tables.

Thank you, great post.

HK9b6a - July 7, 2011, 6:46 am

This isn't new, and it isn't his tutorial. It was originally posted here:

<http://www.explorehacking.com/2011/02/setting-backdoor-in-windows-command.html>

LaCosTa - July 7, 2011, 7:08 am

awesome tutorial dude thanksss !

ilikecheesetwo - July 30, 2011, 6:38 pm

Only works on xp :(didn't work for me

Edit: nvm got it to work silly me thanks

mepsnet - July 30, 2011, 6:53 pm

This way is better:

hackforums.net/showthread.php?tid=1490691

seriosword - July 30, 2011, 6:59 pm

nice i really like this site glad for all your contributions

SkipTheDishes - July 30, 2011, 7:37 pm

Cheers. Will use this when I'm back at school!

Killer_Thriller - July 30, 2011, 9:39 pm

cool worked for me :P..Thanks

danhenrique - October 23, 2011, 6:39 pm

It didn't work for me. I need admin rights to replace the file. But thanks anyway.

Zoom IT - October 23, 2011, 9:22 pm

when i am typing "net user administrator xxx"

it says

system error 5 has occurred

access is denied

i am using windows 7

Sepultra - October 23, 2011, 9:58 pm

when i copy back sethc to sys32 it shows "you dnt have permission to perform this"

bgxcdic - October 23, 2011, 10:59 pm

the computer would have to be pretty fucked to allow the guest account to access system32. A better way that nearly always works is to do the same moving etc, but use a linux live boot distro :D

td james - October 23, 2011, 11:36 pm

thanks for the tut man helped me out alot bro. thanks for sharing.

Handsome Banana - October 24, 2011, 2:17 am

Looks good. But you have to have access to system32 :/

Love Neg Reps - October 24, 2011, 2:19 am

Thanks very help full guide. Changed my self to Admin ^^.

iDuL - October 24, 2011, 11:57 am

I'm sure I can do this easily on my work computer, but getting admin access is not my concern.

Heroicis - October 29, 2011, 2:50 pm

Wow not bad! Is there a way to only find out the admin password without changing it?
~please reply?

crestiage - October 29, 2011, 5:13 pm

Great TUT! Will try it out on my school when classes begin :)

hamid507 - September 22, 2016, 12:05 am

I cant overwrite.... Guess why? COZ I AM NOT AN ADMIN ;)

Mr. Corleone - September 22, 2016, 12:44 am

(Sep 22, 2016 12:05 AM)hamid507 Wrote: [CITE](#) I cant overwrite.... Guess why? COZ I AM NOT AN ADMIN ;)

This tutorial is outdated, Microsoft has long already secured Administrators from having guests do shit like this to them :)