

# RE: How to wreck a computer via a vpn connection and administrator account ?

---

*Source:*

[http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.work\\_remotely/2005-04/msg00234.html](http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.work_remotely/2005-04/msg00234.html)

---

- *From:* v-tomche@xxxxxxxxxxxxxxxxxxxxxxxx (Tom Che [MSFT])
  - *Date:* Fri, 15 Apr 2005 13:31:20 GMT
- 

Hi Skybuck,

Thank you for posting and this is Tom again. :)

>From your post, my understanding of this issue is: How to wreck a computer with Windows XP by logging into it remotely via VPN connection, when the hacker having an Administrator Account of Windows XP is using Windows 98 client. If this is not correct, please feel free to let me know.

To be frank with you, I don't understand why you always suppose that your Administrator Account had been stolen. The Administrator Account is top-drawer for an administrator of a computer or a network, because this account is sovereign in the computer or network. Therefore, the administrator should do his best to protect his account, and had better not empower anybody for anything unless he can be trusted totally.

To protect Administrator Account better:

- 
1. Change the name – If you keep the name the same as the default, this provides 1/2 of the information that an attacker needs to log on as the account. You can change the name to obfuscate the account to novice hackers, such as Mike Lee.
  2. Reset the description – Since the description of the Administrator Account states that it is the default Administrator Account, changing this (or deleting it) will help protect it.
  3. Create a "false" Administrator Account – There are many attackers that are just looking for the name Administrator. So, if you create an account that has no privileges and is even disabled, the attacker will not have a chance to gain access to your network under this account.
  4. Configure a complex password for the account – Observe the following Password Rules:
    - Must be 8 characters long at least.
    - Must have at least 1 capital letter, 1 lower case letter, and 1 number or punctuation, but no spaces.

RE: How to wreck a computer via a vpn connection and administrator account ?

- Cannot be based on your name, NetID, or on words found in a dictionary.
- Cannot be based on simple repeating patterns.

5. If you found any evidence that the Administrator Account had been stolen, you must change the old password immediately.

-----  
Back to your question, if a hacker using Windows 98 logged on your Windows XP with Administrator Account via VPN, he can full control all resources on Windows XP, such as read and write even delete all files just with My Network Places... Is this a "wreck" or not? ;)

I believe that actually you want to protect your computer, so please protect your Administrator Account above all.

Have a nice weekend!

Sincerely,  
Tom Che

Microsoft Online Partner Support  
Get Secure! - [www.microsoft.com/security](http://www.microsoft.com/security)

=====  
When responding to posts, please "Reply to Group" via your newsreader so that others may learn and benefit from your issue.

=====  
This posting is provided "AS IS" with no warranties, and confers no rights.

-----  
>From: "Skybuck Flying" <nospam@xxxxxxxxxxxx>  
>Newsgroups: microsoft.public.windowsxp.work\_remotely  
>Subject: How to wreck a computer via a vpn connection and administrator account ?  
>Date: Thu, 14 Apr 2005 17:55:56 +0200  
>Organization: @Home Benelux  
>Lines: 84  
>Message-ID: <d3m3iu\$atr\$1@xxxxxxxxxxxxxxxxxxxxxxxx>  
>NNTP-Posting-Host: cp250405-a.landg1.lb.home.nl  
>X-Trace: news3.zwoll1.ov.home.nl 1113493918 11195 84.25.126.9 (14 Apr 2005 15:51:58 GMT)  
>X-Complaints-To: usenet@xxxxxxxxxxxx  
>NNTP-Posting-Date: Thu, 14 Apr 2005 15:51:58 +0000 (UTC)  
>X-Priority: 3  
>X-MSMail-Priority: Normal  
>X-Newsreader: Microsoft Outlook Express 6.00.2800.1437  
>X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2800.1441  
>Path:  
TK2MSFTNGXA01.phx.gbl!TK2MSFTNGP08.phx.gbl!newsfeed00.sul.t-online.de!t-online.de!fr.ip.ndsoftware.net!feeder.enertel.nl!nntpfeed-01.ops.asmr-01.energis-idc.net!feeder.xsnews.nl!feeder.news-service.com!newshub2.home.nl!newshub1.home.nl!home.nl!not-for-mail

RE: How to wreck a computer via a vpn connection and administrator account ?

RE: How to wreck a computer via a vpn connection and administrator account ?

>Xref: TK2MSFTNGXA01.phx.gbl microsoft.public.windowsxp.work\_remotely:10933  
>X-Tomcat-NG: microsoft.public.windowsxp.work\_remotely  
>  
>Hi,  
>  
>The question in short is: "How to wreck my own computer by logging into it  
>remotely via vpn connection with an administrator account" ;)  
>  
>Most services are disabled etc (on the host which is windows xp)... ;)  
>  
>Windows 98 <- vpn connection -> Windows XP  
>Bad Hacker Poor victim :)  
>  
>Bye,  
> Skybuck.  
>  
>"Skybuck Flying" <nospam@xxxxxxxxxxxx> wrote in message news:...  
>>  
>> "Tom Che [MSFT]" <v-tomche@xxxxxxxxxxxxxxxxxxxxxxxx> wrote in message  
>> news:bo2V59oPFHA.1960@xxxxxxxxxxxxxxxxxxxxxxxxxxxx  
>> > Hi Skybuck,  
>> >  
>> > Thank you for posting again.  
>> >  
>> > First, I would like to explain that our newsgroup is an issue based  
>> > service, meaning we usually respond to one question/issue per post.  
>> > This  
>> > will lessen the confusion for both of us, as well as ensure that our  
>> > results are accurate and not a result of a test for a different  
>> > question.  
>> > If you have additional question(s), please open a new post so that the  
>> > dedicated MS engineer can help you on it in a more efficient manner.  
>> Thank  
>> > you for your understanding and cooperation.  
>>  
>> Ok, I logged into my own computer as an administrator from another  
>computer  
>> which is running windows 98.  
>>  
>> Windows 98 doesn't have MMC so I guess this theory is now stuck ;) ?  
>>  
>> I did check out these things below locally. I don't see a services  
section  
>> anywhere... so I can't start any services remotely or maybe these can be  
>> started indirectly somehow ;) (?)  
>>  
>> Anyway I looked at all the group policies and stuff...  
>>  
>> But I don't see "Remote Desktop" anywhere...  
>>  
>> I do see other stuff like "Remote Assistance" and "Net meeting" etc.

RE: How to wreck a computer via a vpn connection and administrator account ?

RE: How to wreck a computer via a vpn connection and administrator account ?

>>  
>> I am still interested in finding out if and how someone else with say  
>admins  
>> rights could wreck my computer via a vpn connection ;)  
>>  
>> Bye,  
>> Skybuck.  
>>  
>> >  
>> > To modify GPO remotely, please refer to the following steps:  
>> >  
>> > Step 1  
>> > Click start -> Run, and then input mmc; click OK.  
>> >  
>> > Step 2  
>> > Click File -> Add/Remove Snap-in, and then click Add button in the  
>pop-up  
>> > window. Select Group Policy Object Editor, and then click Add button.  
>> >  
>> > Step 3  
>> > Click Browse button, and then click Computers tab. Select Another  
>> > computer, and then input the computer name you want to modify, or click  
>> > Browse button to find it.  
>> >  
>> > Step 4  
>> > Click OK, and then Click Finish button. Now you can modify this  
>> computer's  
>> > GPO if you have Administrator permission.  
>> >  
>> > Have a nice day!  
>> >  
>> > Sincerely,  
>> > Tom Che  
>>  
>>  
>  
>  
>  
>

---

• *Follow-Ups:*

- ◆ *Re: How to wreck a computer via a vpn connection and administrator account ?*  
◇ *From: Skybuck Flying*

• *References:*

- ◆ *How to wreck a computer via a vpn connection and administrator account ?*  
◇ *From: Skybuck Flying*

RE: How to wreck a computer via a vpn connection and administrator account ?

RE: How to wreck a computer via a vpn connection and administrator account ?

- Prev by Date: [\*\*Re: VPN?\*\*](#)
- Next by Date: [\*\*RD works on LAN not across Internet\*\*](#)
- Previous by thread: [\*\*How to wreck a computer via a vpn connection and administrator account ?\*\*](#)
- Next by thread: [\*\*Re: How to wreck a computer via a vpn connection and administrator account ?\*\*](#)
- Index(es):
  - ◆ [\*\*Date\*\*](#)
  - ◆ [\*\*Thread\*\*](#)