

## Re: User bypasses security

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2005-11/0164.html>

---

**From:** Jim Matthews ([jjmatthews\\_at\\_davtv.com](mailto:jjmatthews_at_davtv.com))

**Date:** 11/17/05

Date: Wed, 16 Nov 2005 20:32:00 -0600

I set up his laptop, using a network share for the source files

As I mentioned, we just went to XP – on Windows 2000, if not logging into the domain, when you reboot you must retype your password, to gain access to persistent shares.

What I have found, with your help, is, that XP allows you to "save" the password over restarts. BUT it saves the username too. Disconnecting the share does not remove the un/password.

Very interesting

JM

"Steven L Umbach" <[n9rou@nospam-comcast.net](mailto:n9rou@nospam-comcast.net)> wrote in message  
news:[uYdJa4v6FHA.252@TK2MSFTNGP15.phx.gbl](mailto:uYdJa4v6FHA.252@TK2MSFTNGP15.phx.gbl)...

> OK. That one seems to catch a lot of us off guard though I don't know how  
> that user got your saved credentials. My guess is that he was a test user  
> account your were using to see how your access policies worked. ---  
> Steve

>

>

> "Jim Matthews" <[jmweb@comcast.net](mailto:jmweb@comcast.net)> wrote in message  
> news:[eYkdf9u6FHA.1420@TK2MSFTNGP09.phx.gbl](mailto:eYkdf9u6FHA.1420@TK2MSFTNGP09.phx.gbl)...

>> Steven – you is da man

>>

>> We are new to XP – his laptop was "caching" my credentials, used to set  
>> it

>> up

>>

>> Many Thanks,

>>

>> JM

>> "Steven L Umbach" <[n9rou@nospam-comcast.net](mailto:n9rou@nospam-comcast.net)> wrote in message  
>> news:[uQbtvZt6FHA.3276@TK2MSFTNGP10.phx.gbl](mailto:uQbtvZt6FHA.3276@TK2MSFTNGP10.phx.gbl)...

>>> Also keep in mind that if you change group membership of a user that you

>>> must logoff and logon as the user again to update the user's security

>> token

microsoft.public.win2000.security: Re: User bypasses security

>>> *with the correct group membership. The support tool whoami can be used*  
>>> *as*  
>> *in*  
>>> *whoami /groups to show the users group membership for the current*  
>>> *security*  
>>> *token. --- Steve*

>>>  
>>>

>>> *"Steven L Umbach" <n9rou@nospam-comcast.net> wrote in message*  
>>> *news:%23g8CFTt6FHA.2176@TK2MSFTNGP14.phx.gbl...*  
>>> *> Jim.*

>>> >

>>> > *When he is connected to the share go to Computer Management/Shared*  
>>> > *Folders – sessions to see as what user he is connected to the folder*  
>>> > *as*

>>> > *and it should also show the source computer. Type 3 logon events would*  
>>> > *also be generated in the security log of the server for the user*  
>> *accessing*

>>> > *the share if auditing of logon events is enabled. If the user is*  
>>> > *different than what you expect then he may be accessing the share with*  
>>> > *credentials other than his own. Windows XP can use "stored*  
>>> > *credentials"*

>>> > *[see link below]to access a server or share though I have no idea how*  
>>> > *he*

>>> > *would have access to your credentials unless you logged on as that*  
>> *account*

>>> > *one time and configured stored credentials. Try having that user logon*  
>> *to*

>>> > *another computer to see if he still can gain access. Also double check*  
>> *the*

>>> > *user's group membership to make sure it is what you expect --- Steve*  
>>> >

>>> >

>>

<http://www.microsoft.com/resources/documentation/Windows/XP/all/reskit/en-us/Default.asp?url=/resources/docume>

>>> >

>>> > *"Jim Matthews" <jmweb@comcast.net> wrote in message*  
>>> > *news:OfeFP6s6FHA.1276@TK2MSFTNGP09.phx.gbl...*

>>> >> *Sorry – he can look at any share and open any file he wishes*  
>>> >>

>>> >> *For example, I have a folder in which I keep confidential info. The*  
>> *only*

>>> >> *share and security permissions on it are me – as Domain Admin and as*  
>>> >> *a*

>>> >> *user.*

>>> >>

>>> >> *He can simply go to Start-->Run and type \\servername and he is shown*

>>> >> *a*

>>> >> *list*

>>> >> *of all shares. If he clicks on my share, he is given access to it all*

>>> >>



microsoft.public.win2000.security: Re: User bypasses security

>>> >  
>>> >  
>>>  
>>>  
>>  
>>  
>  
>