

Re: User bypasses security

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2005-11/0159.html>

From: Jim Matthews (jmweb_at_comcast.net)

Date: 11/16/05

Date: Wed, 16 Nov 2005 14:47:05 -0600

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> wrote in message news: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

> *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

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

> > *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*

> >>

> >> *I have no idea whether he can log on to the server console*

> >>

> >> *Thanks for your help*

> >>

> >> *JM*

> >>

> >> *"Steven L Umbach" <n9rou@nospam-comcast.net> wrote in message*

> >> *news:%23XokZ1s6FHA.3648@tk2msftngp13.phx.gbl...*

> >>> *Define more specifically what you mean by everything with some examples.*

> >> *Can*

> >>> *he logon to the domain controller console? Can he access it's security*

> >> *logs*

> >>> *via Event Viewer? --- Steve*

> >>>

> >>>

> >>> *"Jim Matthews" <jmweb@comcast.net> wrote in message*

> >>> *news:eJ6fdvs6FHA.3588@TK2MSFTNGP15.phx.gbl...*

> >>> > *My setup (partially) a W2K Server (DC) which houses AD, and files, and*

> >>> > *a*

> >>> > *W2K3 Server which houses Exchange and files.*

> >>> >

> >>> > *I set up a new user (without admin rights) and he has access to*

> >>> > *_everything_*

> >>> > *on the W2k Server, but is "restricted" normally on the W2K3 server.*

> >>> >

> >>> > *He is not a member of any admin group or anything like that. I have*

> >>> > *checked*

> >>> > *and rechecked the permissions on several restricted folders.*

> >>> >

> >>> > *He is running XP Pro*

> >>> >

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

> >>> > *I assume that because he is restricted on the W2K3 server that his*
> >>> > *"permissions" are correct, but there is something amiss on the one*
> >> *server*
> >>> >
> >>> > *Can anyone shed some light on this ?*
> >>> >
> >>> > *Many Thanks*
> >>> >
> >>> > *JM*
> >>> >
> >>> >
> >>>
> >>>
> >>
> >>
> >
> >
>
>