

Re: Please help me, it is highly Urgent.....

Re: Please help me, it is highly Urgent.....

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2007-07/msg01307

- *From:* Abhi <Abhi@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Tue, 31 Jul 2007 03:28:00 -0700
-

Herb,

The reason why the threshold is given as 5 is because of security concern. Our domain is banking domain. If the users accounts are getting locked, it won't get unlocked automatically, they have to contact us then we only manually unlcok it. Hope you have understood our concern.

Persistent drive mappings: Persistent drives may have been established with credentials that subsequently expired. If the user types explicit credentials when they try to connect to a share, the credential is not persistent unless it is explicitly saved by Stored User Names and Passwords. Every time that the user logs off the network, logs on to the network, or restarts the computer, the authentication attempt fails when Windows attempts to restore the connection because there are no stored credentials.

Who does net use differ by map network drive from GUI?
Is persistant drive mappings are not recommended?

"Herb Martin" wrote:

"Abhi" <Abhi@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message news:80F3E13B-FB2B-4352-8D25-70FC74C62B47@xxxxxxxxxxxxxxxxxxxxx

Hi All,
We are in Windows 2000 mixed mode. User accounts are on Child domain.
Now
a
days there is a huge increase in the number of account lockout calls that the helpdesk is recieving.
The settings are like this,
Account lockout duration = 0 (an administrator must unlock the account)
Account lockout threshold = 5 invalid logon attempts
Reset account lockout counter after = 15minutes

Re: Please help me, it is highly Urgent.....

Re: Please help me, it is highly Urgent.....

So you have users who can lock themselves out FREQUENTLY with 5 bad attempts within a 15 minute period.

I have tried to use account lockout tools to find out the root cause. I found that subsequent wrong credentials are being passed by the end users but according to them they have typed the password only once, it is also noted that while they are working all of a sudden their accounts are getting lockedout!

They cannot get "locked out" while they are working as they already have their credentials — their account can get locked out but a new authentication/logon would be required to "see that effect".

Either ther users are DOING it, or they have a program (batch, scheduled task, service) running with their credentials which is doing it. This latter seems likely if they can get 5 bad attempts in less than 15 minutes.

Find every program they run which "holds" credentials on their behalf.

I have enabled netlong logging on PDC Emulator but it did not give any hint.
I was also referring to the technet article,

You need to enable "Account Logon Auditing" on all of the DCs. Usually a GPO on the DC OU is the best place.

<http://technet2.microsoft.com/windowsserver/en/library/f3abc878-3eab-4eaf-9bff-9f0d058d4fc3103>
there are a few things I want to clarify,
Article says Many programs cache credentials or keep active threads that retain the credentials after a user changes their password.

Credentials USUALLY means the Security Access Token, not the username and password.

Programs that directly use the "username/password" are NOT fully integrated with Windows and should NOT be doing this — but sometimes we have no choice. (i.e., Regular Programs, not services.)

Re: Please help me, it is highly Urgent.....

Re: Please help me, it is highly Urgent.....

1)How do I find out the applications which are creating problems? May be IE
if the user selects the option save password), can anyone help me in this?

Could be. One way to avoid this is to go strictly to INTEGRATED AUTHENTICATION and ONLY IE (no firefox probably) and the users will be using the Security Token for domain resources on web servers and supplying their password will not be an issue.

Also note that normally IE does NOT (I believe) cache domain logon credentials but only FORM (HTML etc) logons (password/username.)

2)Bad Password Threshold is set too low: This is one of the most common misconfiguration issues. Many companies set the Bad Password Threshold registry value to a value lower than the default value of 10. If you set this value too low, false lockouts occur when programs automatically retry invalid passwords. Microsoft recommends that you leave this value at its default value of 10. For more information, see "Choosing Account Lockout Settings for Your Deployment" in this document.

Threshold, Duration, and Timeout must all be considered together. The lower the threshold then typically the SHORTER the timeout you may wish to use.

What are you trying to prevent? Users from stealing other peoples passwords?
Programs (robots) from discovering passwords?

Almost any password threshold (even 100 or more) will stop the latter.

No such threshold will stop the former if the users are sloppy or otherwise not security conscious.

In our environment Bad Password Threshold is set to 5. But my question is regarding the value 10 which is given in the article. Is there any specific reason why a value of 10 is recommended? and what does it mean by false lockout?

3)Persistent drive mappings: Persistent drives may have been established with credentials that subsequently expired. If the user types explicit credentials when they try to connect to a share, the credential is not persistent unless it is explicitly saved by Stored User Names and

Re: Please help me, it is highly Urgent.....

Re: Please help me, it is highly Urgent.....

Passwords.

Every time that the user logs off the network, logs on to the network, or restarts the computer, the authentication attempt fails when Windows attempts to restore the connection because there are no stored credentials.

Who does net use differ by map network drive from GUI?

Is persistant drive mappings are not recommended?

One more thing I have noticed is that these issues are coming from Windows 2000 professional with SP4, not from XP professional and our DCs are

Windows

2000 with SP4.

Any help and pointers are highly appreciated.