

Re: Domain authenticating non-domain accounts

Source:

<http://www.derkeiler.com/Newsgroups/microsoft.public.platformsdk.security/2008-02/msg00112.html>

- *From:* "Paul Baker [MVP, Windows – SDK]" <paulrichardbaker@xxxxxxxxxxxxxxxxxxx>
 - *Date:* Thu, 21 Feb 2008 14:31:00 –0500
-

Dave,

The problem with doing as you suggest is that I am not a network administrator and I do not have the full support of those that are. I simply want to be able to understand the behaviour of our software as it is presented to me, without going running to them.

Literally, in response to a lengthy email to them I got the response "They're all set". I spoke to them in person and it was like pulling teeth to get the information that what they did is join it to the domain. After that, I wasn't able to pull any more teeth.

Regardless, your answer is useful and appreciated, as it tells me I am not crazy in thinking this very well could be an authentication change that has likely motivations.

I still can't find the darn KB article, to see if it was updated.

Thanks,

Paul

"DaveMo" <david.mowers@xxxxxxxxxx> wrote in message <news:400c053c-b6cd-4063-84a1-13a7ad1c24d0@xx>
On Feb 21, 6:57 am, "Paul Baker [MVP, Windows – SDK]" <paulrichardba...@xxxxxxxxxxxxxxxxxxx> wrote:

We have a single domain and several testing machines on the same network but that are not joined to the domain.

Some years ago, I would routinely create a local account on the testing machine with the same user name and password as that on the domain and when I attempted to access file shares on a machine that is joined to the domain, I would seamlessly be authenticated and the expected access controls applied. I think there is even a KB article explaining that this behaviour

Re: Domain authenticating non-domain accounts

is intentional, that in a sense the domain controller trusts non-domain accounts as long as the user name and password match.

This has not been working the same recently. I limited the tests to Windows

Explorer so I could eliminate something wrong in my code. I simply used Start/Run and \\machinename to attempt to access a machine joined to the domain and, if prompted to logon, I cancelled it so as to avoid any credential caching that might skew results.

Right now, a machine running Windows 98 can still access file shares seamlessly. However, a machine running Windows XP SP2 and one running a beta

version of Windows Server 2008 both exhibit the same problem. Most machines

on the network and joined to the domain (and most run Windows XP) prompted for a logon but were able to authenticate me as long as I entered the same user name and password again, with or without the domain prefix. This used to be seamless. One machine on the network, which happens to be a domain controller (we have two I think), did not prompt for a logon and was seamless. I can understand that maybe we upgraded the version of Windows on

the domain controllers and that the trust relationship is no longer allowed

so as to better protect the domain from unknown machines, but even if that is so, it does not explain why this domain controller was LESS strict about protecting ITSELF.

Many of the testing machines are actually virtual running under Virtual PC, but that is probably not relevant.

My network admin was not able to answer my questions and simply suggested the solution of having him join the testing machines to the domain.

Can someone please offer an explanation?

Thanks for reading,

Paul

Hi Paul,

I am completely guessing, but it could be that MS is closing some loopholes in NTLM authentication with the more recent versions. The old behavior was somewhat of a hack and the powers that be may have come upon a decision point where they could have better security by always prompting. There is always the possibility, of course, that the change in non-joined logon behavior was completely unintentional and

Re: Domain authenticating non-domain accounts

the by-product of some other change.

I have no idea why one of your DCs is acting differently, but I would start by examining policies and patch versions on the two machines that act differently.

Dave

.