

Domain authenticating non-domain accounts

Source:

<http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2008-02/msg00076.html>

- *From:* "Paul Baker [MVP, Windows – SDK]" <paulrichardbaker@xxxxxxxxxxxxxxxxxxx>
 - *Date:* Fri, 22 Feb 2008 09:14:15 –0500
-

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 is intentional (I can't find it), 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.

Domain authenticating non-domain accounts

I have already posted to [microsoft.public.platformsdk.security](#) about this,
but
both replies indicated that they guessed it was change to NTLM
authentication
without confirming what exactly the change was.

Can someone please offer an explanation or point me to where I might find
one?

Thanks for reading,

Paul

.