

Re: NTLM authentication

Source:

<http://www.tech-archive.net/Archive/DotNet/microsoft.public.dotnet.languages.csharp/2007-01/msg00959.html>

- *From:* "Willy Denoyette [MVP]" <willy.denoyette@xxxxxxxxxx>
 - *Date:* Mon, 8 Jan 2007 12:38:43 +0100
-

"webrod" <rodolphe.aoustin@xxxxxxxxxx> wrote in message
<news:1168242607.530464.16420@xx>

Willy,

I am very surprised!!

I have tested with 4 employees in my companies.

My PC is a new one: there is NO local accounts.

They do NOT exist on my PC!!

This is true, this is my OWN PC, I mean I am the person who access this PC and only me.

If I authenticate as I did again ADAM with their login/pwd, it works.

If I enter a WRONG pwd, it doesn't authenticate (so it is the proof that the default authentication type is NOT "None".)

And you can believe me, there is no local users on my PC except: Administrator, admin, ASPNET, IUSR_BW200120, console_de.

You are saying "ADSI know which domain controller stores BOB's credentials?", this is a good question, I guess it knows the domain of the current user so it tries to authenticate BOB with this domain, or I don't know... But it does

Say that the user is "administrator" with password "adminpwd", what administrator would be used to authenticate, the LOCAL admin or the DOMAIN admin,?? According to you it would use the domain administrator, well, I say it's not.

There must be something wrong with your set-up or your code, really.

Please do yourself and us a favor and try to answer the following questions:

- What Framework version are you running on XP?
- Are you logged on into your domain or locally?
- Your DC is running NT4, right? .
- Enable (success and Fail) Logon auditing in your Local Security Policy. Clear the Security EventLog and watch the security events after each bind. Note that this can't be done on NT4, so you can only watch the local logon attempts.
- What happens if you run ldp.exe (from the ADAM prompt) and execute:
Connect to localhost port 389 (the defaults)

Re: NTLM authentication

Bind using NTLM:

enter User (BOB or whatever you consider a valid domain account) and Password, leave Domain empty
press advanced, select NTLM from the list and press OK

press OK in the Bind dialog

This should fail because authentication will be done to the LOCAL SAM and you said BOB is non local (which I believe).

Now try the same specifying the domain name, this should succeed.

– How does your path string look like? Are you sure you specify the port like this:

DirectoryEntry(LDAP://server:389 ...

where server is the server name running ADAM and 389 the port on which the instance is listening (here the default)

– Now, use the "domain\\user" syntax for the username in your DirectoryEntry constructor, where domain is your logon domain (NT4) and user a domain account. This is the syntax that makes it possible for the Security Provider to make a distinction between a local account and a domain account.

– what's the result when running this code?

– and what logon events do you get in your Security log?

Willy.