

Re: LocalSystem service, share, null session, ...

Source:

<http://www.tech-archive.net/Archive/Development/microsoft.public.win32.programmer.kernel/2004-05/0378.html>

From: Pavel Lebedinsky (*m_pll*)

Date: 05/15/04

Date: Fri, 14 May 2004 19:48:42 -0700

In a native Win2K domain the default authentication protocol should be Kerberos, which allows LocalSystem to authenticate over network using the machine AD account (DOMAIN\MACHINENAME\$).

If this is what happens in your case then your service is not actually using NULL sessions – it's authenticating just like any regular account would.

In the case where it doesn't work it could be because the domain is not native Win2K (e.g. you have NT4 DCs), or something else prevents Kerberos from being used.

If you enable auditing of account logons you should be able to get more information in the security event log, such as what authentication protocol is used (kerberos/ntlm), what account is the service trying to authenticate as etc.

"Nicolas Cadilhac" wrote:

> *Hi,*
>
> *this is a tricky problem I have, related to the network (made of w2k*
> *machines). Here it is:*
>
> *On our corporate network, I have a service that I developed that runs as*
> *LocalSystem. This service uses CreateProcess to run a tool that accesses a*
> *remote share. It works, knowing that the share has "everyone" in its*
> *permissions. Maybe the fact that null sessions are allowed helps (I see*
> *that*
> *in the local policies in the administrative tools, or directly in the*
> *registry).*
>
> *On another side, I have a customer that installs my service but the tool*
> *that is ran by CreateProcess fails somewhere (the share is also for*
> *everyone). I wonder if his network configuration is different... When he*

microsoft.public.win32.programmer.kernel: Re: LocalSystem service, share, null session, ...

- > *uses the service as a user, it works. If I give him a standalone version of*
- > *the service ran by the user, it works.*
- > *On my machine where the share is, I tried to disable null session access*
- > *(wanting to reproduce his problem), but the service still continues to work*
- > *while accessing the share !! (a call to net use \\machine\ipc\$ "" /user:""*
- > *fails).*
- > *Why does it continue to work ?*
- >
- > *Except the problem of allowing or not null sessions, what else could I check*
- > *to see differences on both networks ?*
- >
- > *Thanks a lot for your help*
- >
- > *Nicolas*
- >
- >