

Re: Impersonation issue with PsExec ?

Source:

<http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.general/2004-02/4614.html>

From: Drew Cooper [MSFT] (*dcoop_at_online.microsoft.com*)

Date: 02/20/04

Date: Fri, 20 Feb 2004 12:40:53 -0800

If you're running the latest version of psexec, you might want to contact Mark at SysInternals – if any user can connect it sounds like a security bug. Psexecsvc is probably already running as local system (it does on my machine). It uses the user name and password (plaintext – another security problem) parameters to impersonates a different user.

Some options for remote execution of a batch file:

- WMI
- Task Scheduler service

Even better than just a cmdline:

- Remote Desktop/Terminal Services

We might have a kerberized telnet client available now. I know there were folks working on one.

--

Drew Cooper [MSFT]

This posting is provided "AS IS" with no warranties, and confers no rights.

"Yuri Palagin" <ypal@utc.ru> wrote in message

news:O2Wrhd49DHA.1268@TK2MSFTNGP12.phx.gbl...

> Hi there.

>

>

>

> I want to enable some users to use PsExec utility (www.sysinternals.com) for

> executing commands remotely on some servers, but the problem is, PsExec has

> a key "-s" that lets "run remote process in the System account"(as the help

> goes). My testing shows that using "psexec \\server -s cmd" allows any user

> to get access to do just anything on servers with the Admin\$ share on. OK, I

> can disable the Admin\$ share, but this disables using PsExec at all. I got a

> hunch that it has something to do with restricting the right to impersonate,

> but I've no idea where I can find it. Can anyone give me a lead?

>

>

microsoft.public.win2000.general: Re: Impersonation issue with PsExec ?

>
> I'm not stuck with PsExec, so maybe there is another way to allow remote
> command-line to only the chosen, is there?
>
>
>
> Thanks for any ideas,
>
>
> ypal
>
>