

## Re: hacking the logon

**Source:**

[http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security\\_admin/2002-06/2689.html](http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2002-06/2689.html)

---

**From:** Roger Abell ([mvpNOSPAM@asu.edu](mailto:mvpNOSPAM@asu.edu))

**Date:** 06/09/02

From: "Roger Abell" <[mvpNOSPAM@asu.edu](mailto:mvpNOSPAM@asu.edu)>

Date: Sat, 8 Jun 2002 23:58:23 -0700

Jared,

OK, the confusion has cleared. But, I have not encountered a system that shows this behavior. I would speculate that your system has been backdoored in some way. You could try scanning with some product like PestPatrol that looks for known vermin.

Try this. After logging in with this account that has no name, open a command prompt and enter set  
Examine the output for the values of the env vars  
USERNAME and USERPROFILE  
What is it telling you?

I would then use the user management interface to examine the membership of the Administrators group, make sure that I had a couple admins accounts that I knew I could use, and then remove the no-name account from Administrators, if available to do so and possible, and then I would set a new password on the no-name account (again, if I could get at it) and then disable the account. Since XP does not behave this way on its own, you would need to get to the bottom of this. A repair install may replace the system files that have to have been hooked/altered in order for the system to behave this way.

--

Roger Abell

MVP (Windows Platform) Associate Expert

The Expert Zone - [www.microsoft.com/windowsxp/expertzone](http://www.microsoft.com/windowsxp/expertzone)

"jared" <[dresarii@hotmail.com](mailto:dresarii@hotmail.com)> wrote in message

news:c98201c20f20\$c2fff680\$3aef2ecf@TKMSFTNGXA09...

ok, i understand what you are saying on most everything. my

problem is within windows, not the bios, i know that much.

i know this because it occurs at the login prompt/welcome screen by ctrl-alt-deleting as you had said.

but i am still at square one as far as fixing this problem goes.

i know exactly the following because i watched him do it.

when the welcome screen came up, and he was given a choice

microsoft.public.windowsxp.security\_admin: Re: hacking the logon

of users, he hit ctrl-alt-delete, left both the username and password fields blank at the login prompt accessible through ctrl-alt-deleting, and by doing that he logged on to an account with which he created new users. i assume this 'account' has admin rights if it can create new users. so we tweaked with winxp settings, and took the entire welcome screen out, so that a login prompt came up instead. again, we left both the username and password fields blank, and again we logged onto this 'account' and had access to everything.  
how do i prevent this? ive downloaded all security fixes from windowsupdate.com