

Re: Many XP Pro Security Questions – Please Help

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2006-03/msg00276.html

- *From:* "Steven L Umbach" <n9rou@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Sat, 11 Mar 2006 18:13:12 -0600
-

It makes the most sense to create another regular user account that you can logon to. That is what I do. If you use another user account that belongs to another user then you lose accountability for that user. --- Steve

"Jason Antman" <JasonAntman@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message <news:E9CB9AC5-D4C9-4719-A72C-15C91B1516E3@xxxxxxxxxxxxxxxxxxxx>

"Steven L Umbach" wrote:

"Jason Antman" <Jason Antman@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message <news:70D95331-FBE9-402B-8521-43C4BCD8718B@xxxxxxxxxxxxxxxxxxxx>

Hello,

I am now in charge of the computer systems in a volunteer organization.

We

have five Windows XP Pro systems. I am mainly from a Linux/Unix/Windows

2000

environment. There are a few things which I am trying to do to secure

the

computers, but am having problems with:

- 1) I need to have the system create an audit log of all software installations.

There is not an easy way to do this as not all installations get installed

Re: Many XP Pro Security Questions – Please Help

in the program files folder [some get installed in the user's profile where user generally has full control permissions] though you could enable auditing of object access on the computer and then audit only for folder creation to the program files folder but auditing of object access and going through the numerous events in the security log is NOT user friendly. Some installations will show up in the application log particularly for .msi packages.

<http://support.microsoft.com/default.aspx?scid=kb:en-us:300549> --- applies to XP also

2) In the event viewer, there are a number of logins from "ANONYMOUS LOGIN"
What is this, and how do I prevent it?

You will see a lot of that in a workgroup setting and it is normal as "null sessions" are used to build and maintain the browse list that you see and use in My Network Places. It can also mean that you have simple file sharing enabled on the XP Pro computers and users are authenticating as guest to other computer in the network instead of their user account. You can disable simple file sharing in Windows Explorer/tools.folder options/view and uncheck the last option for use simple file sharing. To disable for browse list maintenance you would need to disable file and print sharing on the computer where the events are shown but that may not be an option if you need it.

http://www.practicallynetworked.com/sharing/xp_filesharing/ --- simple file sharing

3) Why does windows XP not show file creator/ownership?
There were a number of programs recently installed on the system, all of which are unauthorized.
How do I find out who created them?

XP should show the owner. The security tab will not be visible until you

Re: Many XP Pro Security Questions – Please Help

disable simple file sharing.

<http://support.microsoft.com/default.aspx?scid=kb:en-us:308418> --- more on NTFS simple file sharing

4) Finally... I have Administrator rights. I want to sign on as a "limited" user. How do I do this? Is there a way to just switch users, or can I somehow get their password?

Just create a user account for yourself that is not in the administrators group and logon with that account. If you want you can use runas to use your administrator credentials to run applications while you are logged on as a regular user. I like to use lusrmgr.msc to manage users and groups rather than Control Panel/users. Right clicking many desktop Icons or program Icons/shortcuts will often show a runas option or you can use runas from the command line. You can also switch users in XP Pro if the computers are not in an Active Directory domain.

<http://www.microsoft.com/windowsxp/using/setup/learnmore/share/fus.mspx> --- Switching users

XP Pro has some very powerful capabilities such as Software Restriction Policies that you can use to manage what applications a user can use or install using path or hash rules starting with a default security level of disallowed or unrestricted. The first link below explains more on SRP and for workgroup computers you may find that the free Microsoft Shared Computer Toolkit is just what you need to lockdown your unprivileged users. --- Steve

<http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/rstrplcy.mspx> --- XP Software Restriction Policies
<http://www.microsoft.com/windowsxp/sharedaccess/default.mspx> --- Shared Computer Toolkit

Re: Many XP Pro Security Questions – Please Help

Thanks,
Jason

Steven,

Thanks for the help. About logging on as another user... what I want to do is log on AS an existing member. I.e. I am an administrator, I would like to work AS one of the user accounts.