

Choose Your Country United States
[Home](#) | [Company](#) | [IT & Management Training](#) | [Enterprise Solutions](#) | [OnDemand Software](#) | [Contact](#)

My Global Knowledge

Quickbuy[Course Catalog](#)[Certifications](#)[Partners](#)[Government](#)[Delivery Methods](#)[Savings Programs](#)[Training Locations](#)[Resource Center](#)[Shopping Cart](#)Search For
Keyword

Go

[Advanced Search](#)**How to... 'Stealth' Microsoft Windows XP Professional**

February 2005 - Tim Warner

In a former position, I worked as a senior-level network engineer for a high-profile research institute at a leading university in the southern United States. Within the institute, there were some Windows XP Professional workstations that hosted top-secret data and, at the same time, required access both to the local area network (LAN) as well as to the Internet. Therefore, my challenge was to harden the security on these computers as much as possible. (I know as much as any security professional does that the only true way to ensure the security of a computer is to remove its connectivity to any network altogether. However, I also understand that in some cases, this measure is impractical and sometimes impossible to implement in practice.)

In this article, I will share some tips for putting a Windows XP Professional-based workstation into "stealth mode." We won't be delving into the intricacies of Internet Protocol Security (IPSec) or hardware firewall traffic policies. Instead, I'll present a series of tips, tweaks and suggestions that you can apply quickly and easily to improve the security of any Windows XP Professional box on your network.

Shall we get started?

TIPS FOR STEALTHING WINDOWS XP PROFESSIONAL—QUICK LOOK

1. Disable File and Printer Sharing.
2. Remove computer from "My Network Places" browse lists.
3. Manually remove administrative shares.
4. Choose a host name that does not identify the computer on the LAN.
5. Secure root volumes.
6. Use a personal firewall.
7. Rely on regular system audits.

Tip 1: Disable the Server Service

The Server service, which is also known as the "File and Printer Sharing for Microsoft Networks" component in Windows XP, can be very dangerous when enabled on a Windows XP computer that is not actually going to host shared resources on a network. In such a case, you would be well advised to open your Network Connections folder, right-click your Local Area Connection, choose "Properties" from the shortcut menu and deselect or entirely remove the "File and Printer Sharing for Microsoft Networks" option. As an added safeguard, open the "Services" Microsoft Management Console (MMC) by typing "services.msc" at the "Run" prompt, and disable the Server and Computer Browser services.

Tip 2: Hide the Computer From Network Browse Lists

Here is a nifty Registry hack that will ensure that your computer will never appear in "My Network Places" browse lists. (Yes, I realize that if you have followed my advice in Tip 1, this tip is rendered largely null and void. However, additional safeguards can only enhance system security.)

Here is the procedure: Open Registry Editor by typing "regedit" at the "Run" prompt. Next, browse to the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer Registry key. Create a REG_DWORD value named "Hidden" and give it a value of "1." This procedure will effectively make your workstation

invisible on NetBIOS browse lists.

Tip 3: Remove the Administrative Shares

Most Windows administrators know that they can access the root volumes of domain workstations and servers by appending a dollar sign (\$) to the drive letter of each root volume's hidden administrative share. For instance, I could use the Universal Naming Convention (UNC) statement \\Server01\c\$ to connect to the root of the C drive of the Windows domain server named "Server01," provided I had the proper domain administrator privileges.

This Registry hack allows you to remove those administrative shares manually from a Windows XP computer that should not have those shares enabled for security reasons. To enable this hack, open Registry Editor and browse to the following Registry key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters

Create two new REG_DWORD values: "AutoShareServer" and "AutoShareWks," and set each value to "0." Restart the computer, and presto-no more administrative shares. You can verify your work by opening the "Computer Management" MMC console, expanding the Shared Folders node, expanding the Shares node and verifying that the hidden administrative shares no longer exist.

Tip 4: 'Mung' the Computer Name and Local User Account Names

Technically, "munging" refers to altering one's e-mail address on Web pages, so it doesn't get picked up by spam harvesters ("tim at hotmail dot com," for example). However, in this context I'll use the term "munging" to refer to choosing a host name for your workstation that in no way, shape or manner serves to identify the computer on your LAN. That is, naming a computer "DATABOX1" probably isn't the best idea in the world if the computer is going to store confidential files. On the other hand, a workstation named "89XYZYX98" is interesting only to a mathematician (due to its palindromic nature).

A shopworn but always-cogent recommendation is to change the names of the two default local accounts: Administrator and Guest. I'll also throw in a plug for choosing strong passwords for both of these accounts. A good password, to my mind, meets the following criteria:

- Includes a healthy mix of letters, numbers and non-alphanumeric characters.
- Is at least six characters long (preferably at least eight characters long).
- Does not include any part of the user's birth name or user name.
- Is not a word that appears in any major language dictionary.

Finally, I would recommend that you disable any local accounts on the computer that will not regularly be used, and log on to the workstation as an administrator only when it is necessary to use administrative privileges.

Tip 5: Secure the Root Volumes

First of all, if the file system in use on your Windows XP Professional workstations isn't already NTFS, then, by all means, please run the "Convert.exe" command-line utility and convert those FAT32 volumes to NTFS, for heaven's sake. Second, ensure that the NTFS permissions on all root volumes are configured appropriately. For instance, it is probably not a wise idea to grant the "Everyone" special group any permissions on any disk volume on a workstation that stores confidential data (although, to Microsoft's credit, Windows XP Service Pack 2 does a pretty good job with setting default NTFS permissions).

On the other hand, be careful not to set NTFS permissions too strictly. To wit, ensure that the SYSTEM special account has the "Allow - Full Control" NTFS permission, or you certainly will have problems with system services failing, as you will be preventing the operating system from accessing its own core files.

Tip 6: Install a Personal Firewall

The personal firewall that is included in Windows XP Service Pack 2 (appropriately called "Windows Firewall") is useful. However, this freebie firewall offers limited configurability and can be used to protect only incoming, not outgoing, connections. You heard me correctly: If your system happens to become infected with malicious code, the Windows Firewall will merrily allow this malicious code to deploy as many packets through your network interface as it wants, assuming that all packets originating from "inside" your computer are trusted.

The solution to this problem is to install a quality personal firewall product. Debates rage among IT professionals as to which product offers the most power, flexibility and protection. I have had great success with Kerio Personal Firewall (www.kerio.com/kpf_home.html). Others can be found through Sygate (www.sygate.com), ZoneLabs (www.zonelabs.com), Agnitum (www.agnitum.com), McAfee (www.mcafee.com) and Norton (www.symantec.com).

Tip 7: Audit Early and Often

System auditing is perhaps the only way in which you can ascertain who is attempting to do what on your system at any given point in time. The Windows Event Log service is pretty impressive, and you can learn quite a bit studying

the event logs by using the "Event Viewer" MMC console. (For even more help in parsing those cryptic event ID codes, visit www.eventid.net.)

However, the good folks at GFI have produced a stellar application that puts the Event Log service and Event Viewer on steroids. You really have to check out the GFI LANguard Security Event Log Monitor application. Visit www.gfi.com/lanselm for more details. For a high-security workstation, an application like this is a must for detailed auditing.

Tim Warner is director of Information Technology for Ensworth High School in Nashville, Tenn. He also owns an Internet security consulting business and teaches computer networking courses in his spare time.

Reprinted Courtesy of [Certification Magazine](#)

Related Global Knowledge Courses

[Microsoft Deploying Group Policy for Windows 2000, 2003, and XP Clients](#)

[Microsoft Windows XP/2003 Server Troubleshooting](#)

[Microsoft Windows XP](#)

Copyright ©2005 Global Knowledge Network, Inc. All rights reserved. [Privacy](#) [Legal](#) [Policies](#)