

by Scott Lowe, MCSE

- 1 Install Service Pack 1** – Windows Server 2003 Service Pack 1 includes a number of key security enhancements, including major improvements to Internet Explorer (useful for a Terminal Services server), a new firewall, a new security configuration wizard designed to help you lock down your server, and the Post-Setup Security Update service, which keeps your system disconnected from the network until such time as you do a Windows Update to make it current. I'd recommend that you slipstream SP1 for new Windows Server 2003 installations so you can take full advantage of the new security features present during installation. For more information about Service Pack 1, read [this summary](#).
- 2 Always use NTFS** – The NT File System, first introduced with Windows NT more than a decade ago, continues to be one of the best ways to lock down a Windows system. It wasn't that long ago that the choice between FAT and NTFS had to be made and was dependent on the applications that would run on the server. These days, it's much more difficult to find an application that won't work with NTFS, and some even require it. NTFS provides granular control over user permissions and lets you give users only the access they absolutely need to a file or folder. If you have an existing server using FAT, convert it to NTFS using the conversion utility included with Windows.
- 3 Only install what you need** – This is the simplest but most important security advice you'll get, and I'm sure you've heard before. The more software and services that you install and run on your server, the larger attack surface you present to those that want to compromise the system. In particular, don't install things like IIS or file/print services on servers that don't need those particular services. IIS, for example, is a favorite target of hackers, and although IIS 6.0 is more secure by default, it's still not as secure as a system with IIS disabled. Also, take advantage of Windows Server 2003's built-in roles to help you appropriately configure your server and its services.
- 4 Isolate the operating system** – One way to protect your server is to make sure that the operating system is the only component installed on a single disk or partition. Separate company files and programs onto other disks or partitions. That way, if a user, or hacker, gains unauthorized access via a hole in another process, he is less likely to be able to gain access to your operating system installation and corrupt it. Of course, this won't protect you in all scenarios, but is an easy way to add another layer of security to your server.
- 5 Use local accounts for services** – While Windows Server 2003 has reduced the need for service accounts in many instances, they are still a necessity for some Windows services and some third party applications. As such, at some point, you'll be creating accounts that allow these products to log into the system. Wherever possible, create these accounts local to the server on which the application runs rather than creating domain accounts. A domain account, if compromised, can be used by hackers to access additional servers in your organization. If you use local accounts, you're more likely to contain the breach to a single server.
- 6 Rename Administrator account and change default installation folder** – The Administrator account and the C:\WINNT and C:\WINDOWS directories are favorite targets for unsophisticated hackers and are often hard-coded into nefarious exploit scripts readily found on the Internet. Even though these methods for gaining access to a system are crude, they are often effective. To stop some of these scripts from being even effective against your systems, rename your Administrator account and install Windows Server 2003 into a directory other than C:\WINNT or C:\WINDOWS.
- 7 Install a virus scanner on the server** – Even if you have antivirus software on your mail servers and on every PC in your organization, you still need one on your servers, particularly on your file servers. If one of your desktop systems doesn't properly update virus signatures on a regular basis, you could wind up with viruses on your server. On a good day, the infected files would just sit there unused, but on a bad day, that file could be opened up on the server, resulting in an infection and potential loss of services. Or worse, it could find a way to self-propagate.

8

Set up a patching schedule and stick to it – Microsoft typically releases a slew of new patches for its products each month. While it's not a great idea to blindly install every patch that comes down the line, ones that are marked critical and could pertain to your environment should be immediately examined and tested in a testing system/lab and deployed as quickly as possible. Today, exploit code for major vulnerabilities is often released in hours rather than in weeks, so it's imperative to patch promptly.

9

Investigate and implement new Group Policy options – Windows Server 2003 SP1 provides administrators with dozens of new Group Policy options to centrally manage the new security features available with SP1. For example, Windows Server 2003 SP1 includes close to 30 Group Policy options just for managing the new firewall. Just about every security option possible is manageable via Group Policy, and that gives you an effective way to provide a locked down computing environment across all of your servers. For a complete list of group policy options, visit Microsoft's [Windows Server 2003 SP1 Group Policy page](#).

10

Download and read the Windows Server 2003 Security Guide – Microsoft has made freely available [this guide](#) that assists administrators in properly locking down Windows servers. From creating a member server baseline to hardening domain controllers to examining various threats and proven countermeasures, this guide is an important, effective tool that should be part of every Windows administrator's security arsenal.



Scott Lowe has held a variety of jobs in the information technology field. Although he has been involved primarily in IT management and network/systems engineering, he has also served as a DBA, help desk technician, and several other job roles. He is currently the IT Director for Elmira College, a small private college located in Elmira, NY.

Additional resources

- Sign up for our [Windows Server 2003 newsletter](#), delivered on Wednesdays
- Check out all of [TechRepublic's newsletter offerings](#).
- [Hacking Windows-Specific Services on Windows Server 2003](#) (TechRepublic)
- [Active Directory: Lock it down in 10 steps](#) (TechRepublic)
- [Windows Server 2003 can snap back from disasters with Automated System Recovery](#) (TechRepublic)

Version history

Version: 1.0

Published: April 26, 2005

Tell us what you think

TechRepublic downloads are designed to help you get your job done as painlessly and effectively as possible. Because we're continually looking for ways to improve the usefulness of these tools, we need your feedback. Please take a minute to [drop us a line](#) and tell us how well this download worked for you and offer your suggestions for improvement.

Thanks!

—The TechRepublic Downloads Team