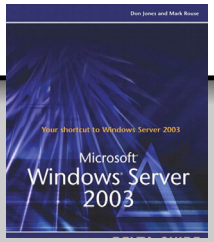
In This Chapter

What's New

Security was a major focus area for Microsoft during the development of Windows Server 2003. In fact, Microsoft created its new Trustworthy Computing initiative during the development of Windows Server 2003 and actually suspended Windows Server 2003's development for two months to focus exclusively on security issues.

As a result, Windows Server 2003 is perhaps the most secure out-of-the-box version of Windows to date. However, that does not mean you can simply install Windows Server 2003 and have a completely secure server. Security is always a trade-off between security and functionality, and you need to configure your servers to strike the appropriate balance for your environment. Windows Server 2003 does make it easier to secure your environment with a variety of security-specific tools, data encryption, and so forth.



Another major security problem Microsoft has tried to deal with over the years is secure code. Viruses, malicious scripts, and other forms of unsecure code have plagued Microsoft operating systems for years. With the release of the .NET Framework, Microsoft has created the first software development environment that incorporates security from the ground up. As software developers move to the .NET Framework for corporate application development, you as a Windows administrator will have more control over the code that executes in your environment, allowing you to prevent malicious code from affecting the productivity of your users.

Microsoft's New Security Philosophy

In mid-2002, an unprecedented series of major security flaws were uncovered in Windows 2000, Internet Explorer 6.0, and IIS 5.0, which are some of Microsoft's most strategically important products. The resulting media backlash resulted in a now-famous "trustworthy computing" internal memo from Bill Gates to all Microsoft employees. The gist of the memo was this: Stop programming and take a look at what you're doing from a security perspective. For two months, production on all Microsoft products stopped, and Microsoft programmers and other employees attended a series of classes designed to highlight common programming practices that often result in security flaws. The programmers also reviewed the code for their products, including Windows Server 2003, with an eye toward removing those unsecure programming practices. The result, according to Microsoft, is that a huge number of security flaws were removed from Windows Server 2003 (and other products) before it was released to manufacturing.

Other practices changed, too. For example, Microsoft products usually go through a beta cycle and then a release candidate (RC) cycle. During the RC phase, new features aren't supposed to be added to the product and major changes aren't supposed to be made. The RC phase is normally designed to catch and fix bugs; any feature that has bugs that can't be fixed is dropped from the product and rolled to the next version's development. For Windows Server 2003, however, the door was left open for security-related changes throughout the product's lifecycle and even into the RC phase. Normally prohibited changes, such as changes to the product's user interface, were allowed if they had a security implication. The message was clear: Deadlines could be missed and features could change if doing so was necessary to prevent security problems in the product.

The new security philosophy resulted in several important changes. For example, IIS has been a major area for security vulnerabilities, due primarily to the fact that IIS is installed by default on all Windows 2000 Server computers. Windows Server 2003 improves its own security by not installing IIS by default and, when IIS is installed by an administrator, using a default configuration that disables many of IIS's more commonly exploited features, such as dynamic Web pages.

Caution The biggest security mistake is complacency. Despite Microsoft's new philosophy and attention to security, Windows Server 2003 has undiscovered security vulnerabilities. Maintaining a secure environment requires constant vigilance, an aggressive program of applying security updates to all computers, and an inherently secure network design. In other words, you should expect a good portion of your time as an administrator to be spent on security and security-related tasks. Don't rely on Microsoft to do your security work for you; investigate potential security holes in your infrastructure and develop ways to protect them.

A major portion of Microsoft's new security philosophy can be reflected in the default configurations for its products. In the past, Microsoft's goal was to provide a default configuration that offered maximum functionality. Now, Microsoft's goal is to provide a more secure default configuration, even at the expense of advanced functionality and features. In other words, Microsoft is willing to provide features that aren't turned on by default and require an administrator to manually enable those features and implicitly acknowledge the features' security implications.

This new philosophy puts a lot more of the security burden on you, the Windows administrator. Before you change any default settings or install any additional components, think about what they'll do to the security of your network. Research settings and components to discover their potential weaknesses and find out how hackers might exploit them to attack your network.

Security Tools

Windows Server 2003 doesn't introduce a lot in the way of new security tools. It does, however, introduce some minor improvements in its tools and includes many helpful tools that are available as add-ons for Windows 2000. For this one section of the book, we're going to veer slightly off our regular course. In general, we're not using this book to explain things that exist in Windows 2000; instead we're saving space to cover just what's new and changed in Windows Server 2003. However, Microsoft's user surveys—and our personal experience—indicates that most administrators have never used many of Windows 2000's security tools. For that reason, we're going to approach the major tools from scratch, showing you how they work and explaining their effects on Windows Server 2003's overall security picture. If you're already familiar with these tools, feel free to skim through the next few sections looking for the bits that have changed.

Note Security isn't a standalone item in Windows Server 2003; it's incorporated throughout the operating system. We've provided a handy list of cross-references at the end of this chapter that direct you to other security-related topics in this book, including Active Directory and IIS.

Security Configuration Manager

You'll see that the Windows Server 2003 documentation refers to the Security Configuration Manager toolset. The phrase itself is a bit misleading because there's no one tool actually named "Security Configuration Manager." Instead, Windows Server 2003 includes a group of related tools—Security Templates, Security Configuration and Analysis, and so forth—that provide security-specific functionality. Windows Server 2003's primary security tools include

- **Security Templates, and Security Configuration and Analysis**—These two MMC snap-ins, which are discussed in the next section, make applying consistent security settings across your organization easier.
- **Security Settings extension to Group Policy**—This tool makes editing the security information on a domain, a site, or an organizational unit (OU) within Active Directory easy.
- **Local Security Policy**—This MMC snap-in edits the security configuration of a local computer, including its password policy and other security settings. A similar snap-in on domain controllers enables you to edit these security properties for an entire domain.
- **`Secedit.exe`**—This command-line tool applies or analyzes security templates. Its non-graphical interface makes it ideal for use in batch files.

Windows Server 2003 includes another tool we especially like, called `Hfnetchk.exe` (which stands for HotFix NETwork CHecKer). `Hfnetchk.exe` is designed to analyze Windows computers and let you know whether they're missing any recent security updates. We cover this tool later in this chapter, in the section "`Hfnetchk.exe`."

Security Templates, Configuration, and Analysis

Configuring Windows Server 2003's security features requires a lot of attention to detail. One of the biggest problems, therefore, is in consistently applying a detailed security configuration across an enterprise. After all, manually configuring a company's computers is time-consuming, not to mention error-prone. To help consistently apply complex security configurations, Windows 2000 introduced the concept of security templates, and Windows Server 2003 makes great use of templates to enable consistent enterprise-wide security.

The idea behind a *security template* is straightforward: Bundle a bunch of security settings into a single file, and then apply that file to multiple computers. In effect, the template is like a security checklist, forcing computers to configure themselves according to a standard you've created. The best—and worst—part about security templates is that they are *cumulative*, which means they can build on one another. For example, you might apply template A to configure your company's baseline security settings and then apply template B to configure department-specific security settings that build on the company's baseline. This flexibility

makes it easier to manage enterprise security with a relatively small number of templates, but it can also make troubleshooting configuration problems a real nightmare because you have to figure out which templates apply each setting.

Tip When you're using security templates, the easiest way to stay out of trouble is to thoroughly document what each template does. That way, you'll be able to easily determine what the end result of several templates will be, and you'll avoid time-consuming backtracking when you have to troubleshoot problems.

To make things easier, Windows Server 2003 offers two MMC snap-ins dedicated to security templates: The Security Templates snap-in and the Security Configuration and Analysis snap-in. Windows Server 2003 doesn't come with a preconfigured console for the snap-ins, so you must open the MMC and add them yourself. We like to add both snap-ins to the same console because they're so closely related. Figure 4.1 shows them in use.

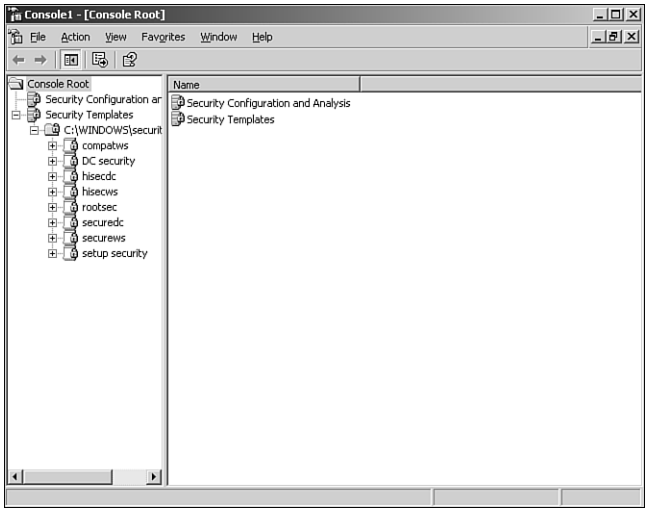


Figure 4.1 Save your custom console for easier use in the future.

Security Templates Snap-in

The Security Templates snap-in is the best place to start. The snap-in starts with a list of the templates that are included with Windows Server 2003:

- **Compatws**—Designed to lower specific file system and Registry permissions to enable some older Windows applications to run properly.
- **DC security**—Designed to be applied to domain controllers, it provides a higher level of security.

- **Hisecdc**—An even more secure configuration for domain controllers, it requires network encryption from clients.
- **Hisecws**—A highly secure configuration that enables IPSec encryption with secure servers. This template can be applied to workstations and member servers in a domain.
- **Securedc**—A slightly less-secure template than Hisecdc, intended for use on domain controllers.
- **Securews**—A slightly less-secure template than Hisecws, intended for use on workstations and member servers.

We don't recommend trying to memorize what these templates do. Instead, consult the Windows Server 2003 documentation for details. You should know, however, that each template configures settings in seven areas:

- **Account Policies**—These policies include password policies, account lockout policies, and Kerberos protocol policies.
- **Local Policies**—These include auditing, user rights, and miscellaneous security options.
- **Event Log**—These policies configure the size and retention behavior for the built-in application, security, and system event logs.
- **Restricted Groups**—These policies define the membership of key user groups, such as the local Administrators group.
- **System Services**—These define the status of services, enabling an administrator to centrally control which services are permitted to run on company computers.
- **Registry**—These policies define security on system Registry keys.
- **File System**—These policies define NT File System (NTFS) security permissions for the entire file system.

For a quick refresher on NTFS file permissions, visit `www.samspublishing.com` and enter this book's ISBN number (no hyphens or parenthesis) in the Search field; then click the book cover image to access the book details page. Click the Web Resources link in the More Information section, and locate article ID# **A010401**.

If you've skipped Windows 2000 and are coming straight from Windows NT, you'll find this article especially helpful because it explains how Windows Server 2003 and Windows 2000 NTFS permissions differ from NT.

As you can see, the list of things you can configure within a security template is quite comprehensive. You can even modify the settings in any of the built-in templates (although we recommend you make a backup copy first, in case you want to revert to the original settings later). Simply double-click any setting to open a dialog box that enables you to change it. Figure 4.2 shows the result of a change to the Hisecws template. Notice how the setting for the Alerter service has been changed to Disabled.

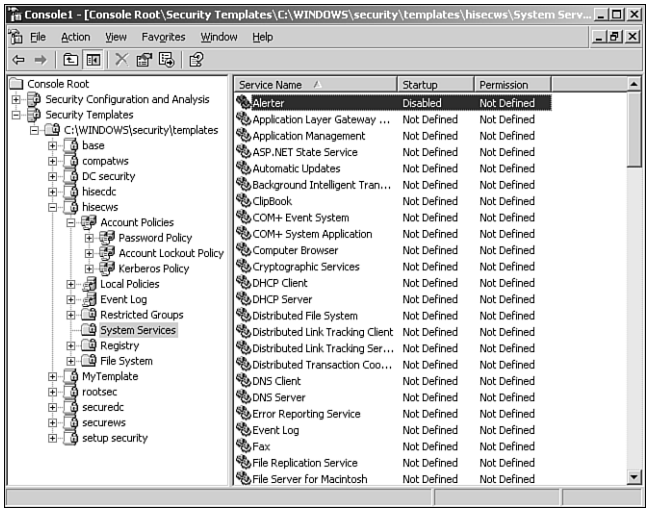


Figure 4.2 To save your changes, right-click the template name and select **Save** from the pop-up menu.

Figure 4.2 also illustrates an important security template concept: *Definition*. Notice in the figure that all services except Alerter are set to Not Defined**.** This setting means the template doesn't actually contain a setting and that applying the template to a computer will not change that particular setting on the computer. If you see something configured as Not Defined in a security template, you know that the template will have no effect on that setting when the template is applied.

If you don't want to start with one of the default templates, you can create your own from scratch. Simply right-click a templates folder, such as `C:\WINDOWS\security\templates` and select **New Template** from the pop-up menu. You'll be asked to provide a name and location for your new template, and then you'll be able to modify its settings, as shown in Figure 4.3. All new templates start out with all their settings undefined, allowing you to customize the template to contain exactly the security settings you want.

After you've created the templates you need, you can deploy them. We'll discuss that next.

Security Configuration and Analysis

Working with templates can be difficult. Although you can use the Security Templates snap-in to see what's in a template, knowing what effect the template will have on a computer is sometimes difficult. The Security Configuration and Analysis (SCA) snap-in is designed to do just that: Show you what effect any given template will have.

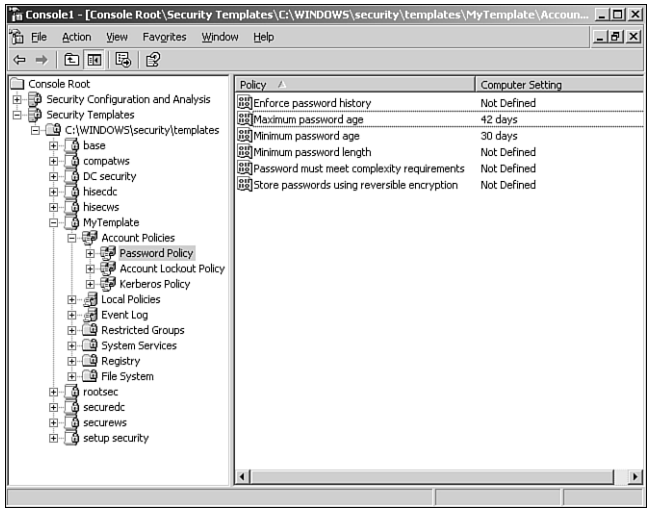


Figure 4.3 Creating your own templates provides maximum security flexibility.

The SCA works with a security database and can create, open, and manage multiple databases so that you can manage different security configurations. A *security database* contains all the settings you want to apply to a computer. SCA includes an import function, so you can import security templates into the database. Figure 4.4 shows the import dialog box, which has a check box in the lower-left corner labeled Clear This Database Before Importing. When this check box is cleared, the import process adds a new security template to the database, layering it on top of whatever's already in there—exactly how security templates work when applied to a computer. When you select the check box, however, the import process first clears the database, starting with a clean configuration. Select the check box when you're ready to begin working with a new database or if you want to wipe out the work you've done so far and start over.

For example, suppose you start with a blank database and import a security template named Template1. Then, you import a second template, named Template2, and you leave the check box cleared. The database will now contain all the settings in both Template1 and Template2. If the two templates contain any conflicting settings, the ones in Template2 will be effective. If, on the other hand, you had selected the check box when importing Template2, the database would contain only the settings in Template2. Everything from Template1 would have been cleared out prior to the import.

After you've imported one or more security templates into a database, you can *analyze* the database against the computer. The analyze process compares the settings in the database to the active configuration of the current computer, without actually applying those settings. The result, shown in Figure 4.5, enables you to easily see exactly what effect the database's

settings will have. Figure 4.6 shows additional analysis details. Notice how SCA uses icons to highlight settings in the database that don't match the computer's current configuration. Were you to actually apply the template to the computer, those settings would be changed. Settings that aren't defined in the database, or settings that are defined in the template and currently configured on the computer, aren't called out with a special icon.

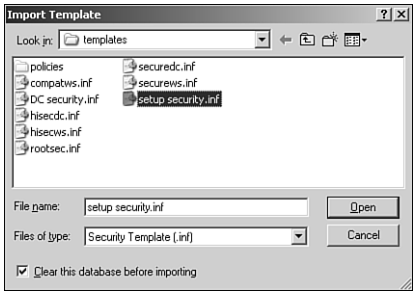


Figure 4.4 You can import multiple security templates into a single security database.

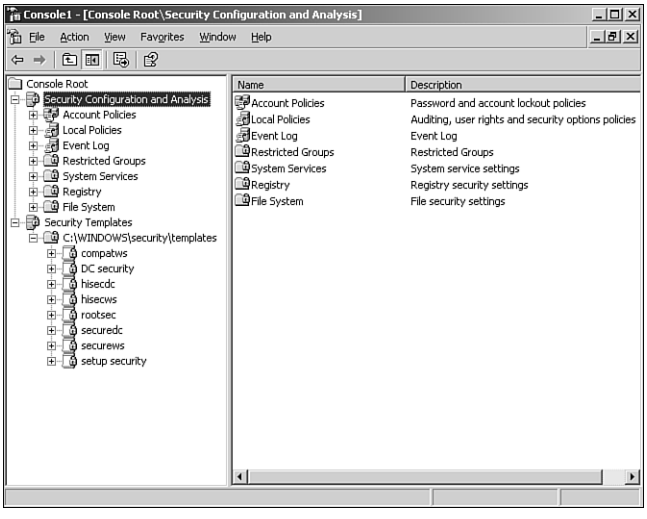


Figure 4.5 Analyzing lets you easily see the effect that one or more security templates will have on a standard computer configuration.

You can also make changes to the security database manually, without the use of a template. The process is similar to modifying a security template: Simply double-click the setting you want to change. Different types of settings present different dialog boxes. For example,

Figure 4.7 shows what a file security setting looks like, whereas Figure 4.8 shows a password policy setting. You can remove a setting from the database by clearing the check box that defines the policy in the security database.

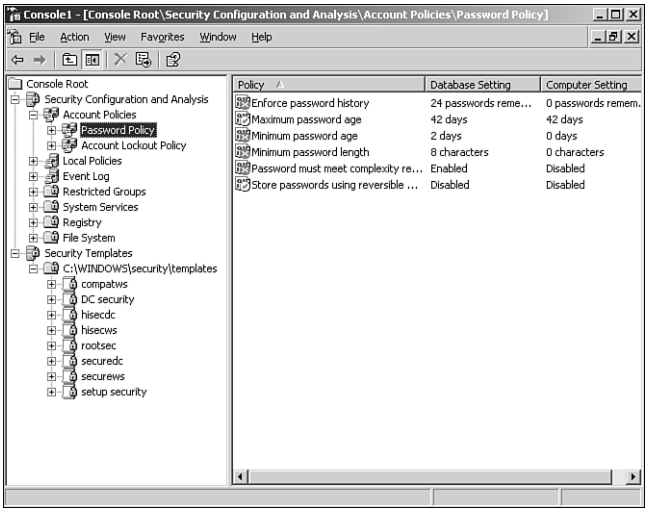


Figure 4.6 Special icons call your attention to differences between the security database and the current configuration.

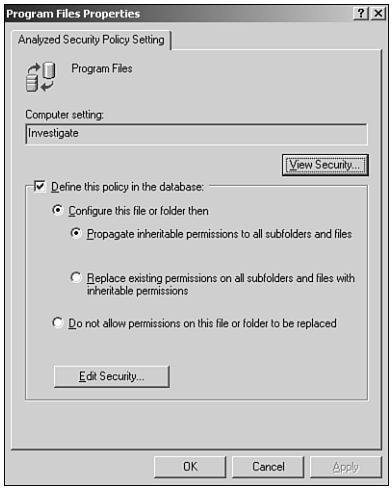


Figure 4.7 Use a security database to specify file permissions.

Figure 4.8 Use a security database to specify a password policy setting.

After you've configured your security database exactly the way you want it—either by importing the desired security templates or by manually configuring the database—you have two options for deploying the settings. The easiest is to simply apply the database directly to the computer by right-clicking the **SCA** snap-in and selecting **Configure** from the pop-up menu. Doing so applies the current database to the local computer's active configuration, making the two match. You can also export the database into a security template, which is a bit easier to deploy automatically throughout your enterprise.

Tip Windows Server 2003 also includes `Secedit.exe`, a command-line tool introduced in Windows 2000. `Secedit.exe` can be used to import security templates into a database, analyze databases, and configure the local computer. One way to deploy security settings is to deploy a preconfigured security database and use `Secedit.exe`—perhaps in a batch file—to apply that database to the local computer.

Perhaps the easiest way to deploy security settings in an Active Directory domain is by using Group Policy. With Group Policy, you can create a new Group Policy object (GPO); import a security template (either one of the included templates or one you created); and link the GPO to a site, an OU, or a domain. All computers contained in that site, OU, or domain will receive the new security settings within an hour or so. Keep in mind that the standard order of group policy application applies: Site policies first, followed by domain policies, and then OUs.

Caution Not all Windows operating systems support the same security features. Windows 2000 and Windows XP offer slightly different features, so you probably should maintain individual security templates for each operating system. Applying a security template intended for one operating system to a different version can potentially have devastating effects, so be sure to test your templates and apply them only where appropriate.

Hfnetchk.exe

Hfnetchk.exe is a free download from Microsoft's Web site (www.Microsoft.com/download). Hfnetchk was actually developed by an outside firm, Shavlik (www.shavlik.com), and licensed to Microsoft; you can purchase a more fully functional version directly from Shavlik. The commercial version of the tool includes a complete graphical user interface; Microsoft's free version is strictly a command-line tool. Both of them, however, work similarly.

Note Hfnetchk is documented in Microsoft Knowledge Base article Q303215 (http://support.Microsoft.com/default.aspx?scid=kb;en-us;Q303215). You can learn more about the commercial version at http://www.shavlik.com.

Hfnetchk is driven by an XML-based security database, which the tool can download directly from Microsoft. This database describes the latest security updates (formerly known as *security hotfixes*) available from Microsoft, including service packs. The database also describes the specific changes each security update makes to the operating system, especially to files and Registry keys. These descriptions enable Hfnetchk to analyze your computer and determine exactly which security updates have, or have not, been correctly applied. Hfnetchk produces a comprehensive report that tells you exactly which updates you should obtain and apply. Most importantly, it can run across a network, analyzing remote computers to which you have administrative permissions.

Hfnetchk is a useful tool to have in your security arsenal, and it's a tool you should run on a regular basis, especially against security-critical servers such as firewalls and domain controllers. Keep in mind, however, that Hfnetchk is primarily a *reactive* tool, which means it can alert you only to existing security problems. An enterprise-wide deployment of a more proactive solution, such as Software Update Services (SUS), can ensure that your computers always have the latest security updates applied. You can then use Hfnetchk in more of an auditing role to ensure that SUS is working properly and that security updates are, in fact, being applied as intended.

Encrypting Data

Similar to Windows 2000, Windows Server 2003 supports the Microsoft Encrypting File System (EFS), which enables users and administrators to encrypt files using Windows strong built-in encryption capabilities. *Encryption* provides an extra level of security over file permissions: Even if the server is compromised and someone gains access to encrypted files, he won't be able to use the files without the appropriate decryption key.

Windows Server 2003 takes EFS one step further than Windows 2000, however, incorporating multiple-user access (a feature already present in Windows XP). Under Windows 2000, only the user who encrypted a file, or a designated recovery agent, can decrypt a file; in Windows Server 2003, users and administrators can designate other users to have decryption

capabilities. To access the new feature, right-click any encrypted file and select **Properties** from the pop-up menu. Then, select **Advanced** in the Properties dialog box and click **Details** next to the check box that enables encryption. You'll see a dialog box similar to the one in Figure 4.9, in which you can manage the users who can access the file.

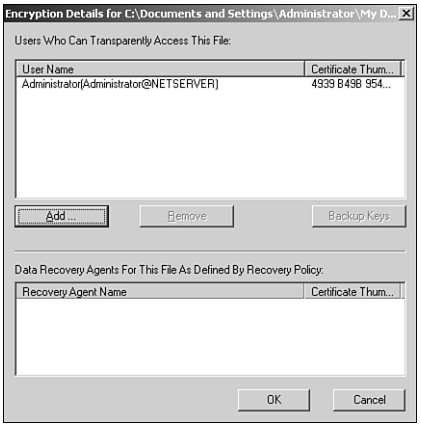


Figure 4.9 Adding multiple users is great for departments that need to protect files while still providing access for multiple users.

Note Keep in mind that EFS doesn't encrypt folders. You can designate a folder for encryption, but that simply tells Windows to individually encrypt each file within the folder. As a result, you can't assign multiple decryption users on a folder; you have to make the assignment on the files themselves. You can, however, highlight multiple files in Explorer and change their properties all at once.

Windows Server 2003 also provides complete support for encrypting network data via the IPSec network security protocol, Secure Sockets Layer (SSL) encryption for HTTP and other protocols, and so forth. For more information on these security options, see the cross-reference list at the end of this chapter.

Common Security Holes

Have you thought about how the network services in your environment might be used against you and how Windows Server 2003's components offer features to protect your network? A good *security administrator*—a role that is increasingly recognized as a standalone job task within larger environments—has to be constantly paranoid. Even the most seemingly innocent and beneficial network services can be used against you. The next few sections cover some examples to get your paranoid juices flowing. Windows Server 2003 provides options to secure

almost all the services against common security attacks, but you'll have to take it upon yourself to implement more secure configurations. Although Windows Server 2003 is more secure out of the box than any previous version of Windows, some security configurations require a trade-off in functionality, so they're not always included in the defaults.

DNS

DNS is your network's phone book, providing a means for computers to resolve easy-to-remember computer names to more functionally useful IP addresses. Windows Server 2003 provides a Dynamic DNS (DDNS) service, which accepts dynamic DNS record registrations from computers that have dynamic IP addresses. DDNS ensures that all computers can be accurately listed in the DNS database. DDNS, however, provides a potential security flaw: If an intruder can insert a bogus DNS record, she can redirect legitimate traffic to a different computer. For example, if an intruder were able to replace the IP addresses of a domain controller, she could easily gain access to authentication traffic and potentially user passwords.

Fortunately, the worst-case scenarios are pretty hard to imagine. Windows's Kerberos protocol helps ensure that client and server computers can validate one another's identities, making it nearly impossible for intruders to capture traffic (at least, between Windows 2000 and higher computers; older Windows versions don't use Kerberos and can be fooled into sending traffic to an unintended computer).

Intruders could still insert new records into DDNS, however, and potentially use those records in an attack against your network. In fact, when you create a new zone Windows Server 2003's DNS service warns you that allowing just any old dynamic updates is a significant security vulnerability, as shown in Figure 4.10. The DNS service does offer an option for secure updates that accepts updates only from computers that have successfully authenticated to the domain. However, the secure option is available only when the DNS service is running on an Active Directory domain controller, thereby providing DNS with access to authentication information. For that reason alone, we always recommend that your DNS servers also be Active Directory domain controllers and that you enable DNS to use secure DDNS updates.

When you install the DNS service on a Windows Server 2003 computer, a new DNS-specific event log is added, along with the built-in application, security, and system event logs. A regular part of your maintenance routine should be to analyze the DNS log for potential security problems such as a large number of unauthenticated update attempts, which can indicate a potential security attack.

Dynamic Host Configuration Protocol

Dynamic Host Configuration Protocol (DHCP) doesn't offer many security vulnerabilities because its only task is to hand out DHCP addresses. However, some especially secure organizations, including banks and government agencies, often take steps to deny DHCP services to network intruders. By preventing DHCP from providing an IP address to unknown computers,

intruders have that much harder a time working on the network. Of course, an intruder can always make up an IP address; finding one that will work and that isn't already in use can take time, though, and might discourage some attackers.

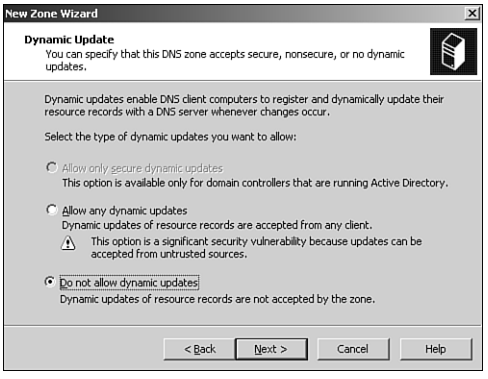


Figure 4.10 Secure updates are possible only on a domain controller.

Securing DHCP in this fashion requires that you configure your computers to use DHCP and then configure DHCP with a reservation for each computer. By ensuring that each DHCP scope contains just enough addresses to fulfill your reservations, you ensure that no extra computers will be capable of obtaining addresses. Of course, using reservations in this fashion largely defeats the "dynamic" part of DHCP; what you're really doing is reverting to static IP configurations that are centrally managed on the DHCP server. This isn't a step most organizations feel is necessary, but it's available as an option if your organization needs to use it.

Network Monitor

Network Monitor (NetMon) is a network packet-capture tool included with almost every version of Windows since Windows NT (it's not included with Windows 9x versions). We won't go into NetMon's operations in detail; the product has been around since early versions of Windows NT and is also included in Microsoft Systems Management Server. What you need to be aware of is how NetMon can be used to compromise network security.

NetMon captures and displays raw network data, meaning anyone with NetMon can analyze practically anything that crosses your network. The most obvious concern, then, is it giving attackers the ability to pick up passwords from your network. For domain authentication, that's not a worry because even older versions of Windows NT and Windows 9x use some pretty powerful encryption techniques. However, for any internal Web sites, FTP sites, or other services that might not use Windows-integrated authentication, password stealing is a very real problem. NetMon also makes pulling other confidential information across the network relatively easy. For example, if someone in your human resources department copies a salaries

spreadsheet to a file server, an intruder could capture the traffic with NetMon and reassemble what should have been confidential information.

Microsoft helps prevent NetMon abuses in a couple of ways. First, the version included with Windows captures only traffic sent to or from the machine on which NetMon is running. That limits the user to capturing whatever is coming and going from his own computer, so he won't likely pick up anything he couldn't have accessed otherwise. However, the so-called "full" version of NetMon, included with Systems Management Server, can pick up anything that passes on the network segment, making it a much more dangerous tool. The full version isn't actually hard to come by apart from Systems Management Server; several Microsoft Official Curriculum courses in the past included it, and several less-than-legitimate Web sites make it available for download.

Fortunately, Microsoft anticipated that unauthorized use of NetMon might be a problem. Every running copy of NetMon sends out occasional packets in a special protocol called *bone*. The protocol name is actually something of an in joke: NetMon's product code-name is "Bloodhound," so naming its internal protocol "bone" is intended to be cutesy. The practical use of the bone protocol is that it enables you to see other copies of NetMon running on your network. You should regularly run the full version of NetMon (yes, you'll probably need to purchase Systems Management Server to get a legal copy) and check for bone broadcasts from other copies. To do so, follow these steps:

1. Perform a network capture with NetMon. Let it run for several minutes, at least.
2. View the completed capture and add a new filter by clicking the **Filter** icon in the toolbar.
3. Double-click the filter's **Protocol** line and disable all but the bone protocol, as shown in Figure 4.11.

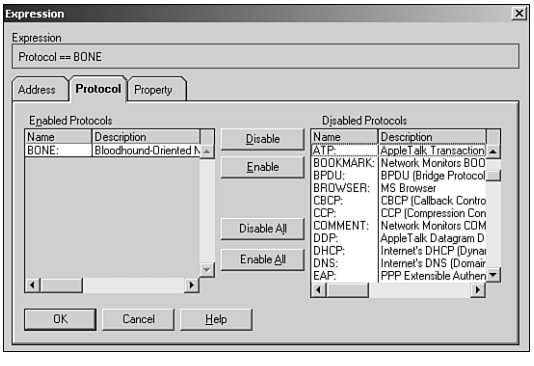


Figure 4.11 Disabling all but bone makes spotting bone packets in a large capture easier.

4. Close the dialog box, and ensure that your filter looks like the one in Figure 4.12.

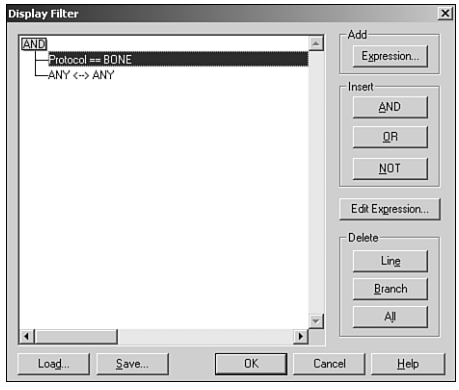


Figure 4.12 A properly configured filter makes spotting bone broadcasts without missing any important data easier.

5. Review any packets shown in the capture. Bone packets include the IP address of the computer that sent it, helping you to track down the unauthorized user.

Caution Don't see any bone frames in your capture? Don't relax. Even the full version of NetMon can capture only the traffic on your local network segment, so you'll need to perform a capture on each segment. In a switched environment, you can usually configure your switches to forward all traffic to one switch port, where you can plug in your NetMon computer to capture everything.

Finally, keep in mind that NetMon is not a unique product. Even though it's relatively easy to acquire, plenty of other commercial packet sniffers are available that an attacker can use to pull information from your network as it passes by on the wire. Not all these other products include something similar to the bone protocol, so you won't be able to detect their use. The best way to keep these packet capture tools under control is to firmly control what software your users can run on their computers and to guard all physical connections to your network that an intruder might use to gain access.

Internet Information System

IIS has come to be known as one of Microsoft's more serious security flaws, primarily because it's installed by default on so many operating systems. Several viruses, including the now-famous "Code Red" worm, attack IIS directly, set up shop on the attacked computer, continue to attack other computers from there, and eventually spread throughout the network.

Although IIS isn't installed by default on Windows Server 2003, it's still the default option on older versions of Windows. You can go a long way toward securing your environment by removing IIS from computers on which it isn't necessary and by applying the latest service packs and security updates to computers that must run IIS. A vigorous antivirus plan, including frequent updates to virus definitions, can help protect both servers and clients from viruses that attack IIS.

Developing a Security Strategy

As we've mentioned a couple of times already, security is not something you worry about once and never again. It's a constant process, and to make that process as efficient as possible, you need to have a battle plan. We find that the ongoing work of security falls more or less into two areas: auditing and maintenance. That's not to say no other security-related tasks exist; on the contrary, most of what we cover in this book is security configuration. But configuration is more of a one-time thing: You configure some security settings and you're done. Auditing and maintenance, however, are two security-related tasks that are never finished.

Auditing

Auditing is the process of reviewing something—in this case, security-related somethings—to ensure they comply with some standard. Windows Server 2003 provides several types of auditing:

- **You can configure auditing on file and folder access**—This enables you to review who is accessing files. This auditing takes place in the security event log, and you have to decide which files and folders to audit.
- **You can audit domain events such as user logons**—As with file access, you have to decide which events to audit, and the events themselves are listed in the security event log.
- **You can audit IIS log files to look for errors, potential security problems, and much more**—You have to configure IIS to create a log file, and you must manually review the log. It's just a text file (not a regular event log), although you can purchase third-party applications to help summarize log information and call your attention to possible problems.
- **You can audit the DNS log**—This is included in the Event Viewer snap-in. This log can alert you to potential security problems as well as operational errors.

Of course, there are many more. You should also make it a regular habit to audit things other than logs. For example, you might occasionally look at the membership of your company's Enterprise Admins, Domain Admins, and Schema Admins user groups. The members of these groups have powerful built-in permissions, and an occasional check to ensure the groups contain only authorized users is a good practice. Your organization might set up other sensitive groups, and you should check them on a periodic basis, too.

Auditing can be a daunting task, with so many things to look at. Consider creating a checklist that helps you remember which things to look at.

Tip Remember, only you can prevent forest fires and only you can prevent security breaches. Microsoft has given Windows Server 2003 the capability to be as secure as you need it to be; it's your job to implement those capabilities and to ensure they continue to meet your organization's ongoing needs.

Security Maintenance

Unfortunately, securing your servers isn't a one-time task. Hackers are constantly finding new ways to compromise common security measures, and you'll always need to implement new measures to maintain your environment's security levels. Also, despite Microsoft's Trustworthy Computing initiative, rest assured that Windows Server 2003 does contain bugs, and some of those bugs will affect the product's security. As those bugs are discovered and squashed, you'll need to apply the appropriate fixes to your servers. Bear in mind that Microsoft offers a few types of fixes:

- **Service packs**—These roll up several months' worth of fixes, along with new features, into a single, cumulative package. Each service pack contains all prior fixes, so that installing service pack 2, for example, also installs the fixes contained in service pack 1. Service packs go through an extensive beta-test cycle and are fully regression-tested, so they shouldn't introduce new bugs. In practice, of course, Microsoft rarely releases a perfect service pack; we recommend waiting a few weeks after the release of a new service pack to ensure it's relatively well-behaved.

Note One of the reasons service packs can be buggy is that Microsoft uses them to deploy new features. Every so often, Microsoft resolves to stop doing that and to include only bug fixes. To my knowledge, that has never actually happened and service packs continue to introduce new features and changes to existing features along with a host of bug fixes.

- **Hotfixes**—Also called *quick-fix engineering updates (QFEs)*. These generally correct very specific bugs in the operating system and don't receive the benefit of a full beta-test cycle. Microsoft recommends that you install a hotfix only when you're experiencing the specific problem the hotfix addresses. We concur with this recommendation; don't treat hotfixes as something you casually deploy because they can sometimes break things. If you're not experiencing the specific problem the hotfix solves, wait until the next service pack. Every service pack rolls up the preceding hotfixes and tests them in a full beta-test cycle.
- **Security updates**—These are basically hotfixes that address security issues. One supposes that Microsoft puts a bit more effort into testing these than a typical hotfix, but because security updates are nearly always released too quickly to fix a problem, don't assume a full beta-test cycle has been completed. Nonetheless, given that they fix

security holes, you should regularly apply the latest security updates and just take the risk that they might break something, too. SUS can help automate security update deployment to Windows 2000, Windows XP, and Windows Server 2003 computers.

In short, your security maintenance plan must include constant vigilance, constant updates, and constant education about new threats. You can start by signing up for Microsoft's Security Bulletin, a free periodic email newsletter, at `www.Microsoft.com/security`.

➤ For more information on using Software Update Services, **see** Chapter 14, "Maintenance," **p. 231**.

➤ For an overview of the Framework, **see** Chapter 9, "Web Development," **p. 145**.

➤ For more information on software restrictions, **see** Chapter 13, "Management," **p. 215**.

➤ For details on how IIS has been made more secure, **see** Chapter 7, "Internet Information Services," **p. 101**.

➤ To learn about Active Directory changes, including Active Directory's role in security, **see** Chapter 5, "Active Directory," **p. 65**.

➤ To see what's new and changed in Group Policy, **see** Chapter 6, "Group Policy Changes," **p. 81**.