Hardening Windows

Second Edition

Jonathan Hassell

Apress®

Hardening Windows, Second Edition

Copyright © 2006 by Jonathan Hassell

ISBN (pbk): 1-59059-539-4

Printed and bound in the United States of America 9 8 7 6 5 4 3 2 1

Lead Editor: Jim Sumser
Technical Reviewer: Oris Orlando
Editorial Board: Steve Anglin, Dan Appleman, Ewan Buckingham, Gary Cornell, Tony Davis, Jason Gilmore, Jonathan Hassell, Chris Mills, Dominic Shakeshaft, Jim Sumser
Associate Publisher: Grace Wong
Project Manager: Kylie Johnston
Copy Edit Manager: Nicole LeClerc
Copy Editor: Liz Welch
Assistant Production Director: Kari Brooks-Copony
Production Editor: Katie Stence
Compositor: Pat Christenson
Proofreader: Elizabeth Berry
Indexer: Toma Mulligan
Interior Designer: Van Winkle Design Group
Cover Designer: Kurt Krames
Manufacturing Director: Tom Debolski

Distributed to the book trade worldwide by Springer-Verlag New York, Inc., 233 Spring Street, 6th Floor, New York, NY 10013. Phone 1-800-SPRINGER, fax 201-348-4505, e-mail `orders-ny@springer-sbm.com`, or visit `http://www.springeronline.com`.

For information on translations, please contact Apress directly at 2560 Ninth Street, Suite 219, Berkeley, CA 94710. Phone 510-549-5930, fax 510-549-5939, e-mail `info@apress.com`, or visit `http://www.apress.com`.

The information in this book is distributed on an “as is” basis, without warranty. Although every precaution has been taken in the preparation of this work, neither the author(s) nor Apress shall have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the information contained in this work.

The source code for this book is available to readers at `http://www.apress.com` in the Source Code section.

CHAPTER 4

Windows XP Security

The advent of always-on connections and the increase of business connectivity to the Internet have resulted in Windows XP computers being directly connected to the Internet, which is a hotbed of potentially dangerous people and computers. In this chapter, you'll look at ways to specifically protect your Windows XP computers from threats that reside abroad.

One note from the beginning about coverage in this chapter: Microsoft has released Windows XP Service Pack 2 (SP2), which is a very broad and very comprehensive set of fixes, functionality updates, and feature introductions that harden Windows XP systems quite well. If you apply XP SP2, then over half of your work is done (enjoy your break): particularly for new installations, the service pack introduces a new set of secure defaults that lessens the need for you to run around targeting security settings for change. I'm going to assume in this chapter that you're running XP SP2; if I'm giving instructions that apply only to a previous level of Windows XP, I'll say so explicitly.

Note The topics in this chapter can also apply to Windows 2000 systems, and the topics in the Windows 2000 chapter can apply here, unless explicitly stated that a topic is only for one of the two. So be sure to consult Chapter 3 for more advice.

Implementing the Built-In Windows XP Firewall

It's simply a given that on Windows XP, you should install a firewall. If you have a case of the cheaps, you should use the included Windows Firewall to control access to services running on the machine. It's a simple process to configure the Windows Firewall, and by doing so you harden the exterior interfaces to the machine from public access. To examine and configure your firewall settings, follow these steps:

1. From the Control Panel, open Security Center.

2. Click Windows Firewall.

Windows Firewall (WF) includes the General, Exceptions, and Advanced tabs. On the General tab, you can turn the firewall on, choose whether to enable exceptions, or turn the firewall off. If you select Don't allow exceptions, the firewall will block all requests to connect to your computer, including requests from programs or services that are listed on the Exceptions tab (which I'll describe in a bit). It will also block both the discovery of network devices and file and printer sharing. You can still, however, browse the network and view web pages normally, as well as send and receive email or use instant messenger (IM) programs.

The Exceptions tab lets you add program and port exceptions to permit certain types of inbound traffic. You can set a scope for each exception. For example, to add a program, click Add Program and then, from the list, select the program you wish to except. You can also click the Change Scope button on the exception list to allow this program to be unblocked for a range of computers, a single host, or the entire network. Similarly, you can add a port by clicking the Add Port button, entering the name of the protocol and the port number you're allowing, specifying whether the protocol is TCP or UDP, and then clicking OK. You can change the scope of a port exception in exactly the same way as a program exception by clicking the Change Scope button on the Add a Port screen.

On the Advanced tab, you can configure connection-specific rules that apply to any network card or virtual interface, the configuration for logging security-related events, the ICMP (ping) acceptance or rejection rules, and a reversion to Windows XP's default firewall configuration if you've bungled your setup.

Profiles

In the WF, Microsoft introduced the concept of *profiles*, which are like hardware profiles in that they represent the configuration of the firewall depending on its current environment and connectivity situation. WF allows for two profiles:

- The standard profile, which is used by default in workgroup environments—that is, XP machines that do not participate in a domain—and simply rejects all incoming traffic

- The domain profile, which is used by default on machines joined to a Windows domain and allows exceptions to be made for inbound and outbound traffic based on services and applications that you have installed

The settings in the standard profile are typically more restrictive than the domain profile's settings because you wouldn't have the services and applications necessary to participate in a domain—this profile is great for traveling laptops that connect from hotel rooms, coffee shops, and other wide-open Internet access terminals.

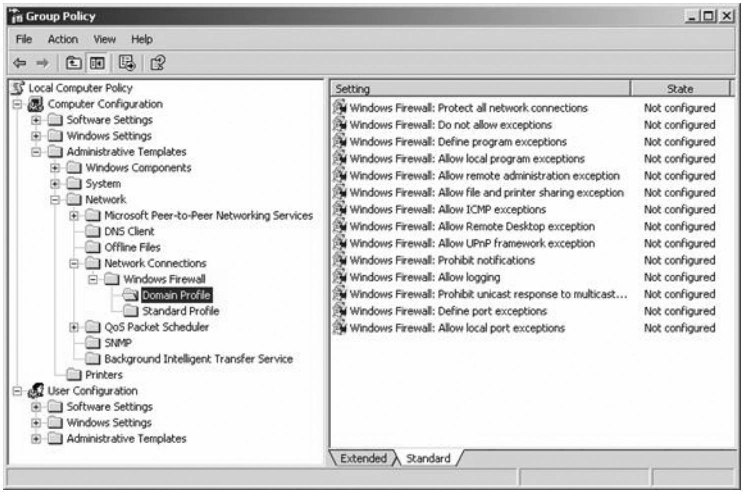
You should ensure that you configure settings for both profiles as soon as possible unless you are not connected to a domain. That way, your security is established from the beginning. You can determine which profile the WF is using by opening the Windows Firewall applet from Control Panel ➤ Security Center and looking at the bottom of the General tab. The text will read “Windows Firewall is using your domain settings” or “Windows Firewall is using your standard settings” in each situation. If you’re interested in doing this from the command line, you can run the following command to accomplish the same thing:

```
Netsh firewall show currentprofile
```

Configuring Through Group Policy

If you’re running Windows XP in an Active Directory environment, you can configure WF through Group Policy (GP), which is a great way to establish a consistent configuration across all of your systems. If you are deploying your first XP SP2 system, you’ll need to run the Group Policy Object Editor from one XP SP2 machine to update the set of GPOs available across your domain—once you do this, you can perform GP configuration from any domain-participating workstation, no matter the operating system.

The new GPOs are shown in Figure 4-1. Note that there are two configuration folders, one each for the domain profile and the standard profile.



Setting	State
Windows Firewall: Protect all network connections	Not configured
Windows Firewall: Do not allow exceptions	Not configured
Windows Firewall: Define program exceptions	Not configured
Windows Firewall: Allow local program exceptions	Not configured
Windows Firewall: Allow remote administration exception	Not configured
Windows Firewall: Allow file and printer sharing exception	Not configured
Windows Firewall: Allow ICMP exceptions	Not configured
Windows Firewall: Allow Remote Desktop exception	Not configured
Windows Firewall: Allow UPnP framework exception	Not configured
Windows Firewall: Prohibit notifications	Not configured
Windows Firewall: Allow logging	Not configured
Windows Firewall: Prohibit unicast response to multicast...	Not configured
Windows Firewall: Define port exceptions	Not configured
Windows Firewall: Allow local port exceptions	Not configured

Figure 4-1. *New GPOs for Windows Firewall*

The Internet Connection Firewall in XP Gold and Service Pack 1

If you’re not yet running XP SP2, then you’ll have to use the Internet Connection Firewall (ICF), which is not as nice and easy to configure as its more modern counterpart but which is still reasonably effective. To configure the ICF, do the following:

1. Open Control Panel, and double-click Network Connections.

2. Double-click the connection that refers to your external interface. The connection status window appears.

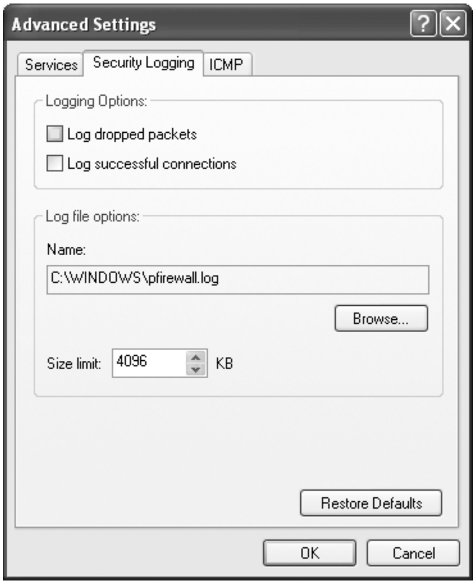
3. Click the Properties button.

4. Navigate to the Advanced tab, and select the box titled Protect My Computer and Network by Limiting or Preventing Access to This Computer from the Internet.

5. Click OK.

Your computer is now protected by the ICF. You can also click the Settings button on the Advanced tab to open specific ports for certain services you might be running.

You should also enable ICF logging on critical computers directly connected to the Internet. Doing so will provide you with an audit trail for later forensic analysis; you can automatically see what changes a hacker or cracker may have made to your system so you can reverse them efficiently. To enable logging, navigate to the Security Logging tab in the Advanced Settings dialog box, as shown in Figure 4-2.



Logging Options:

☐ Log dropped packets

☐ Log successful connections

Log file options:

Name: C:\WINDOWS\pfirewall.log

Size limit: 4096 KB

Figure 4-2. *Enabling ICF security logging*

You can choose whether to log successful connections and packets that are dropped because of firewall rules, and you can also specify a custom location for the log file itself.

■ **Tip** Another reason to upgrade to XP: NT 4 is at the end of its life. Users should plan an upgrade to Windows XP or 2003. Users of Windows 2000 Professional (the desktop version) should consider an upgrade to Windows XP if only for the ICF filtering provided.

If you have a small business or home business network connected to the Internet, the most cost-effective way to obtain the most protection possible for your dollar is to purchase a broadband router, such as those manufactured by Linksys, D-Link, NETGEAR, and others. Most of these units even have built-in switches, and you simply connect each client to the router and the computers are automatically protected—by default—from the outside. Of course, this strategy won’t be as effective when your computing base grows, but it’s an efficient solution for a small business or home business.

Disabling Unnecessary Services

One of the easiest ways for crackers to exploit holes in your system is through open services. In addition to the security benefits you get from auditing and closing unused services, you receive a performance enhancement because stagnant programs aren’t taking up available resources. Besides, a full security audit of your service can reveal some interesting details about your machine. Lately, viruses have been masquerading as services listed in the Task Manager, making them harder to detect, clean, and prevent.

Windows XP comes with only a few services that require open access to an external interface for normal operation: Terminal Services, or Remote Desktop Connection, and the Remote Access Service for answering dial-in calls.

To manage services on your computer, do the following:

1. Right-click My Computer, and choose Manage.

2. Expand the Services & Applications tab, and select Services.

3. Double-click a service.

4. Under Startup Type, select Manual to disable a service from automatically starting upon computer bootup. Click the Stop button to stop the service if it’s already running.

Table 4-1 contains a nearly complete list of all services that ship with Windows XP and the recommended state that each should be in on your computer, assuming normal office functions are being performed on the machine.

Table 4-1. *Common Services and Recommended Settings*

Service Name	Description	Recommended State
Alerter	Raises administrative alerts for selected users and computers.	Disabled.
Application Layer Gateway Service	Required if you use Internet Connection Sharing (ICS) or XP's included Internet Connection Firewall to connect to the Internet.	Automatic if using ICS; disabled if not.
Application Management	Used to assign, publish, and remove software through Group Policy.	Disabled unless you participate in an Active Directory domain.
Automatic Updates Services	Used to check if any critical updates are available for download.	Requires Cryptographic to be running. Automatic if you don't wish to use Windows Update manually.
Background Intelligent Transfer Service	Used by Windows Update to transfer data in the background using otherwise idle available network bandwidth.	Disabled.
ClipBook	Enables the ClipBook Viewer to create and share data to be viewed by remote computers.	Disabled.
COM+ Event System	Provides automatic distribution of events to subscribing programmatic components.	Disabled.
COM+ System Application	Provides automatic distribution of events to subscribing programmatic components.	Disabled.
Computer Browser	Maintains an up-to-date list of computers on your network, and supplies the list to programs that request it.	Disabled.
Cryptographic Services	Confirms signatures of Windows files. Required for Windows Update to function in manual and automatic mode, and required for Windows Media Player as well.	Automatic.
DHCP Client	Manages network configuration by registering and updating IP addresses and DNS server information.	Automatic if required; disabled if not.
Distributed Link Tracking Client	Maintains links between the NTFS file system files within a computer or across computers in a network domain.	Disabled.

Service Name	Description	Recommended State
Distributed Transaction Coordinator	Coordinates transactions that are distributed across multiple computer systems and/or resource managers, such as databases, message queues, file systems, or other transaction-protected resource managers.	Disabled.
DNS Client	Resolves and caches DNS names. The DNS client service must be running on every computer that will perform DNS name resolution.	Automatic.
Error Reporting Service	Calls home to Microsoft when errors occur.	Disabled.
Event Log	Logs event messages issued by programs and Windows. This can be useful in diagnosing problems.	Automatic.
Fax Service	Enables you to send and receive faxes. Disabling this service will render the computer unable to send or receive faxes.	Disabled; or don’t install from distribution media.
Telephony	Provides Java Telephony API (TAPI) support for programs that control telephony devices and IP-based voice connections on the local computer and through the LAN on servers that are also running the service.	Disabled unless required.
FTP Publishing Service	Not available on Windows XP Home. Not installed by default on Windows XP Pro. Enables FTP service.	Disabled; or don’t install from distribution media.
Help and Support	Required for Microsoft’s online help documents.	Automatic.
Human Interface Device Access	If all your devices function, then disable it.	Disabled.
IIS Admin	Not available on Windows XP Home. Not installed by default on Windows XP Pro. Allows administration of Internet Information Services (IIS).	Disabled; or don’t install from distribution media.
IMAPI CD-Burning COM Service	Used for the “drag-and-drop” CD-burn capability. You’ll need this service to burn CDs.	Automatic.

Continued

Table 4-1. *Continued*

Service Name	Description	Recommended State
Indexing Service	Indexes contents and properties of files on local and remote computers and provides rapid access to files through a flexible querying language.	Disabled.
Internet Connection Firewall and Internet Connection Sharing	Provides network address translation (NAT), addressing and name resolution services for all computers on your home or small-office network through a dial-up or broadband connection.	Automatic if sharing connection, disabled if not required.
IPSEC Services	Manages IP security (IPsec) policy, starts the Internet Key Exchange (IKE), and coordinates IPsec policy settings with the IP security driver.	Disabled.
Logical Disk Manager	Watches Plug & Play events for new drives to be detected and passes volume and/or disk information to the Logical Disk Manager Administrative Service to be configured. If disabled, the Disk Management snap-in display will not change when disks are added or removed.	Manual.
Logical Disk Manager Administrative Service	See previous item's description.	Manual.
Message Queuing	A messaging infrastructure and development tool for creating distributed messaging applications for Windows.	Disabled; or don't install from distribution media.
Message Queuing Triggers	Required only if you use Message Queuing Service.	Disabled; or don't install from distribution media.
Messenger	Sends and receives messages to or from users and computers, or those transmitted by administrators or by the Alerter Service.	Disabled.
MS Software Shadow Copy Provider	Used in conjunction with the Volume Shadow Copy Service. Microsoft Backup uses these services.	Enabled.
NetMeeting Remote Desktop Sharing	Allows authorized users to remotely access your Windows desktop from another PC over a corporate intranet by using NetMeeting.	Disabled.

Service Name	Description	Recommended State
Network Connections	Manages objects in the Network and Dial-Up Connections folder, in which you can view both network and remote connections.	Automatic.
Network DDE	Useless service unless you use remote ClipBook.	Disabled.
Network DDE DSDM	See previous item's description.	Disabled.
Network Location Awareness (NLA)	Required for use with the Internet Connection Sharing Service (server only).	Disabled unless running ICS or ICF.
NTLM Security Support Provider	Enables users to log on to the network using the NTLM Authentication Protocol. If this service is stopped, users will be unable to log on to the domain and access services. NTLM is used mostly by Windows versions prior to Windows 2000.	Automatic.
Performance Logs and Alerts	Configures performance logs and alerts.	Disabled.
Plug & Play	Enables a computer to recognize and adapt to hardware changes with little or no user input.	Automatic.
Portable Media Serial Number	Retrieves serial numbers from portable music players connected to your computer.	Disabled.
Print Spooler	Queues and manages print jobs locally and remotely. If you don't have a printer attached, then disable.	Automatic.
Protected Storage	Provides protected storage for sensitive data, such as private keys, to prevent access by unauthorized services processes or users.	Disabled.
QoS RSVP	Provides network signaling and local, traffic-control functionality.	Disabled unless required by your network administrator.
Remote Access Auto Connection Manager	Creates a connection to a remote network whenever a program references a remote DNS or NetBIOS name or address.	Disabled.

Continued

Table 4-1. *Continued*

Service Name	Description	Recommended State
Remote Access Connection Manager	Creates a network connection.	Automatic if using Dial-Up Networking; disabled otherwise.
Remote Desktop Help Session Manager	Manages and controls Remote Assistance.	Disabled.
Remote Procedure Call (RPC)	Provides the endpoint mapper and other miscellaneous RPC services.	Automatic.
Remote Procedure Call Locator	Manages the RPC name service database.	Disabled.
Remote Registry Service	Not available on Windows XP Home. Allows users to connect to a remote registry and read and/or write keys to it—providing they have the required permissions.	Disabled.
Removable Storage	Manages removable media drives and libraries. This service maintains a catalog of identifying information for removable media used by a system, including tapes, CDs, and so on.	Disabled.
RIP Listener	Not installed by default.	Disabled; or don't install from distribution media.
Routing and Remote Access	Offers routing services in local area and wide area network environments.	Disabled; or don't install from distribution media.
Secondary Logon	Allows you to run specific tools and programs with different permissions than your current logon provides.	Automatic.
Security Accounts Manager	Startup of this service signals other services that the Security Accounts Manager subsystem is ready to accept requests.	Automatic.
Server	Provides RPC support and file print and named pipe sharing over the network. The Server Service allows the sharing of your local resources (such as disks and printers) so that other users on the network can access them.	Automatic if you're sharing files; disabled if not.
Shell Hardware Detection	Used for the autoplay of devices like memory cards, some CD drives, and so on.	Disabled unless required.
Simple Mail Transport Protocol (SMTP)	Transports email across the network.	Disabled; or don't install from distribution media.

Service Name	Description	Recommended State
Simple TCP/IP Services	Implements support for a number of IP protocols.	Disabled; or don’t install from distribution media.
Smart Card	Manages and controls access to a smart card inserted into a smart card reader attached to the computer.	Disabled unless using a smart card reader.
Smart Card Helper	Provides support for earlier smart card readers attached to the computer.	Disabled unless using a smart card reader.
SNMP Service	Allows Simple Network Management Protocol (SNMP) requests to be serviced by the local computer.	Disabled; or don’t install from distribution media.
SNMP Trap Service	Receives trap messages generated by local or remote SNMP agents and forwards the messages to SNMP management programs running on the computer.	Disabled; or don’t install from distribution media.
SSDP Discovery Service	Used to locate UPnP devices on your home network.	Disabled.
System Event Notification	Tracks system events such as Windows logon network and power events.	Disabled.
System Restore Service	Creates system snapshots or restore points for returning to at a later time.	Disabled.
Task Scheduler	Enables a program to run at a designated time.	Disabled unless absolutely required.
TCP/IP NetBIOS Helper Service	Enables support for NetBIOS over TCP/IP (NetBT) service and NetBIOS name resolution. Only required if you need to share files with others.	Disabled unless sharing is enabled.
TCP/IP Printer Server	Used for setting up a local UNIX print server.	Disabled; or don’t install from distribution media.
Telephony	Provides Telephony API (TAPI) support for programs that control telephony devices and IP-based voice connections on the local computer and through the LAN on servers that are also running the service.	Disabled.

Continued

Table 4-1. *Continued*

Service Name	Description	Recommended State
Telnet	Allows a remote user to log on to the system and run console programs by using the command line.	Disabled; or don't install from distribution media.
Terminal Services	Provides a multisession environment that allows client devices to access a virtual Windows 2000 Professional desktop session and Windows-based programs running on the server.	Disabled; or don't install from distribution media.
Themes	Used to display all those new XP themes and colors on your desktop. Lots of space needed.	Automatic or manual, depending on your preferences.
Uninterruptible Power Supply (UPS)	Manages communications with a UPS connected to the computer by a serial port.	Disabled unless using a UPS.
Universal Plug & Play Device Host	Used in conjunction with SSDP Discovery Service, it detects and configures UPnP devices on your home network.	Disabled.
Upload Manager	As with BITS, this service manages file transfers between clients and servers on the network. This service is NOT required for basic File and Print sharing.	Disabled.
Volume Shadow Copy	Used in conjunction with the MS Software Shadow Copy Provider Service. Microsoft Backup uses these services.	Disabled.
WebClient	Disable this for security reasons.	Disabled.
Windows Audio	Used to produce audio.	Automatic.
Windows Image Acquisition (WIA)	Used for some scanners and cameras. If, after disabling this service, your scanner or camera fails to function properly, enable this service.	Disabled.
Windows Installer	Installs, repairs, or removes software according to instructions contained in MSI files provided with the applications.	Manual.

Service Name	Description	Recommended State
Windows Management Instrumentation (WMI)	Provides system management information. WMI is an infrastructure for building management applications and instrumentation shipped as an integral part of the current generation of Microsoft operating systems.	Automatic.
Windows Management Instrumentation Driver Extension	Tracks all of the drivers that have registered WMI information to publish.	Manual.
Windows Time	Sets the computer clock. W32Time maintains date and time synchronization on all computers running on a Microsoft Windows network.	Automatic.
Wireless Zero Configuration	Automatic configuration for wireless network devices.	Disabled.
WMI Performance Adapter	Optimizes the speed of WMI queries.	Disabled.
Workstation	Provides network connections and communications. If this service is turned off, no network connections can be made to remote computers using Microsoft Networks.	Automatic.
World Wide Web Publishing Service	Provides HTTP services for applications on the Windows platform.	Disabled; or don’t install from distribution media.

As you can see from Table 4.1, not very much is actually needed to keep your Windows XP installation functioning in a nondomain environment. Most of the enabled services just pose an unfavorable security risk compared to the reward, bring little or no benefit, consume resources, and can be safely turned off.

Providing a Secure Configuration for Services

While disabling unnecessary services is an excellent, and fundamental, step to hardening Windows, there are some other necessary items to accomplish to further secure the services that remain and any services that you may add in the future. Peruse the following list of best practices and consider implementing them:

- **Give strong passwords to service accounts**. When you install applications that require services to be run, you are typically given the option to choose an account under which the service is to be run. Use 15+ character passwords, and remember that you must set these passwords both in Active Directory Users and Computers or Computer Management (depending on your operating environment) *and* in the Log On tab of the service's property sheet.

- **Never let users log on using service accounts**. This most particularly applies to the Administrator account—never assign the Administrator account to a service, and never distribute any service account name and password to any users. There is absolutely no reason to do so, and if users can access systems in these contexts, they can wreak more havoc than you might be able to imagine. Just don't do it.

- **Do not allow network access to service accounts**. For one, this means don't create domain accounts for services; wherever possible, use a local account on the server where the service is located. Also, check the Deny Access to this Computer from the Network right within the service account's property sheet to eliminate network access for that account.

- **Use accounts of least privilege for service accounts**. Windows XP includes a great set of built-in accounts, collectively called the Network Service and Local Service, which are specifically designed to be used for services that require different amounts of network connectivity. Use these where possible to decrease the attack surface of services.

Microsoft Baseline Security Analyzer Patch Check and Security Tests

Windows Update is a good way to update a few computers on your network, but it's a bad strategy for a large network because it requires user intervention and isn't easily automated. As you'll discover in Chapter 9, Microsoft has a better way to automate patch rollout on more than a handful of computers using its Software Update Services package. However, neither option offers a good, sweeping way of determining the update level of your machines.

To fill this need, Microsoft has issued the Baseline Security Analyzer (MBSA) tool, which will query each machine on your network and detect which available patches haven't been installed. The tool is simple to use, easy to automate, and is more suited to a mass analysis than Windows Update. However, it lacks the intelligence and logic of its web-based counterpart. You'll probably see a lot of updates that don't pertain to your machines, even though they aren't installed. It's up to you to verify that the specific patch listed in the results from the MBSA session doesn't apply to specific machines on your network. You'll also need to reboot after each patch application.

Installing Microsoft Baseline Security Analyzer

To install MBSA, follow this procedure:

1. Go to `http://www.microsoft.com` and search for HFNetChk. (I would include a direct URL, but Microsoft has a tendency to change its website around quite often.)

2. Download, execute, and install the program to C:\hfnetchk.

3. At the command prompt, enter **hfnetchk –z –v.**

The –z and –v switches tell the MBSA tool to go out and download a database of all available patches. It will then scan a computer or set of computers for patches that haven't been installed, and indicate which haven't been installed along with the Microsoft Knowledge Base article number. You can look up the appropriate patch using the number provided by the MBSA at `http://www.microsoft.com/support`.

Penetration Tests

Many security vendors provide free or low-cost online tools that evaluate the security of your system, of course with the underlying motive of persuading you to buy their product. These tools are most often a "penetration test" that can indicate how effectively you've hardened your system.

Symantec offers its security check, as well as other tools, at `http://security.symantec.com`. Here you can scan for holes in your computer's external interfaces—a very basic penetration test—or scan for viruses that might be present on your system, and track a cracker's location if you have his source IP. If you've followed the steps in this chapter so far, I highly recommend taking advantage of the Scan for Security Risks option to ensure that you haven't missed anything. In addition to probing your open ports, the option can also detect some Trojan horse viruses that can invade your computer and open a back door.

There's one thing you should be aware of: Each of these Symantec tools download to your system Active X content, which of course should at least give a competent, astute administrator pause. It's up to you to trust a particular vendor. Generally, the more popular security-testing sites will have the most robust scanning tools.

Steve Gibson, of the venerable Gibson Research Corporation, has also made available the popular ShieldsUp! test at `http://www.grc.com`. It performs much the same function as the Symantec tools.

File System Security

Part of hardening your overall XP system is to ensure that your file system is adequately secured. Microsoft provides NT File System (NTFS) support in Windows XP. NTFS allows for more robust security features and user permissions and also adds some basic fault tolerance, with which the older FAT file system just cannot compete. Make sure all of your hard drives are formatted with NTFS unless you have systems that dual-boot to another, older operating system that doesn't support NTFS on the same disk.

To check your hard drive partitions, do the following:

1. Log in as Administrator, and double-click My Computer.

2. Right-click each hard drive letter and choose Properties.

3. Navigate to the General tab. Here, Windows will identify the file system type.

Follow the previous steps for each drive letter, noting which ones are labeled FAT or FAT32.

To convert a FAT or FAT32 partition to NTFS, do the following:

1. Open a command prompt.

2. At the command prompt, enter **convert *x*: /FS:NTFS /V.** Replace *x* with one of the drive letters you noted previously.

3. Repeat the previous step for each FAT or FAT32 partition.

When you've finished, reboot the system for the changes to take effect.

You might also choose to use third-party disk conversion utilities, like PartitionMagic or Norton Disk Doctor, to convert your file system to NTFS. It's a painless procedure, no matter which tool you use to do it. Of course, you should always remember to back up your data before performing any change to a disk's configuration or function.

Disable Automated Logins

Windows XP offers a feature for machines that aren't participating in a security domain where accounts without passwords can automatically log in at a computer's startup without requiring any user intervention. Obviously, this is a huge security hole for machines connected to any kind of network. You'll want to disable this.

To disable automated logins, do the following:

1. Inside Control Panel, open Administrative Tools.
2. Double-click Local Security Policy.
3. Select a username.
4. Make sure there is a password set for each user account that's enabled.

Hardening Default Accounts

The main premise is that in order for someone to access an XP system, she must have a username and password. To that effect, Windows creates the Administrator account, for use by the machine's owner, and a Guest account, which has limited privileges and is designed for people who don't have continuing business on a machine. This isn't just an XP function.

Of course, crackers have taken advantage of the presence of both accounts. You might consider renaming the two accounts to reduce the surface vulnerability of the machine. This doesn't work for server machines all the time; sometimes server software and services require the Administrator account to be named the same, but for client machines, renaming is usually a good strategy. This is true particularly for XP computers, because they tend to be directly connected to the Internet more than computers that are running older versions of Windows.

You can configure the Administrator account as follows:

1. Log in as Administrator.
2. Go to the Control Panel, double-click Administrative Tools, and then double-click Computer Management.
3. Open Local Users and Groups.
4. Click the User folder.
5. Right-click the Administrator account, and choose to rename it. Make it a less obvious name.
6. Right-click this renamed Administrator account and select Set Password.

You can configure the Guest account as follows:

1. Right-click the Guest account, and choose to rename it. Make it a less obvious name.
2. Right-click this renamed Guest account, then select Set Password.

For security reasons, the Guest account in XP is disabled by default. Enabling the Guest account allows anonymous users to access the system. Even if no one sits down and logs in as a guest to your system, the account is used. If you share a folder, the default permission is that everyone has full control, and because Guest is included within the built-in Everyone group, a hole is opened. A standard practice is to always remove the share permissions from Everyone and add them to Authenticated Users. This is a much safer configuration.

Use Runas for Administrative Work

One of the most fundamental laws of security is that you, as the administrator, should use the account of least privilege whenever possible. If you are doing day-to-day work that doesn't require special privileges or powers, then use a regular user account just like the other people in your organization.

Microsoft understood this principle and integrated a convenience feature (yes, security and convenience can meet in a satisfying way in a few instances) called Runas, which allows you to execute applications and programs in a security context other than your current one. So you can run as a normal user in a regular, limited-privilege account, and then access Active Directory Users and Computers using the Runas feature under your administrator credentials. To use Runas:

1. Find the application you want to use in Windows Explorer.
2. Hold down the Shift key and right-click on the application's executable.
3. Click the Run As option.
4. Select The Following User, and then enter the credentials of the alternate account as appropriate.
5. Click OK.

You can also use Runas from the command line. For example, you can create a shell with administrator credentials with the following command, issued from Start ➤ Run:

```
Runas /user:jhwnxpltp\administrator cmd
```

You'll be prompted for the password to the JHWNXPLTP\Administrator account.

Disable Infrared Transfers

Nearly all modern notebook computers have the capability to use infrared for file transfers and other communications—supposedly a convenience tool that allows users to synchronize data with their personal digital assistants (PDAs), music devices like iPods, and other mobile hardware. However, the ability to introduce files into a machine through the air presents an interesting, if yet unexploited, attack vector that should be closed for all but the most knowledgeable users.

In Control Panel, open the Wireless Link applet, and then disable Allow Others to Send Files to Your Computer Using Infrared Communications. While Windows by default would open a pop-up balloon when someone tried to initiate a file transfer, sometimes you can't trust users to select the right option.

Using Forensic Analysis Techniques

Part of hardening a system is knowing when your efforts haven't protected against or prevented an attack. Here are some common indicators that your system has been compromised:

- A system alert, alarm, or related indication from an intrusion-detection tool
- Suspicious entries in system or security logs in XP's Event Viewer

- Unsuccessful logon attempts
- New user accounts of unknown origin
- New files on the physical file system of unknown origin and function
- Unexplained changes or attempt to change file sizes, checksums, timestamps, especially on files within the C:\WINNT or C:\WINDOWS hierarchy (depending on whether the system was upgrading from a previous release of Windows or simply installed from scratch)
- Unexplained addition, deletion, or modification of data
- Denial of service activity or inability of one or more users to log in to an account, including admin or root logins to the console
- System crashes
- Poor system performance
- Unauthorized operation of a program or the addition of a sniffer application to capture network traffic or usernames or passwords
- Port scanning and the use of exploit and vulnerability scanners, remote requests for information about systems and users, or social-engineering attempts
- Unusual usage times; statistically, more security incidents occur during non-working hours than any other time
- An indicated last time of usage for an account that doesn't correspond to the actual last time of usage for that account
- Unusual usage patterns; for example, programs are being compiled in the account of a user who doesn't know how to program

Keep alert for these indicators. If any are tripped, back up any personal data on a machine, verify that data's integrity, and then reformat the machine and reinstall Windows. It isn't a safe bet to try to reconstruct a compromised machine for later production use.

Checkpoints

If you're in a hurry, the action items within this chapter include the following:

- Upgrade to Windows XP Service Pack 2 as soon as possible.
- Use XP's included Windows Firewall (or the Internet Connection Firewall if you're not yet running XP Service Pack 2) to close off open ports.
- Configure Windows Firewall profiles explicitly to provide the best security from the beginning.
- Enable ICF logging for later forensic analysis and intrusion detection.
- If you have a small office or home office network, purchase an inexpensive broadband router for further protection.
- Adjust your running services list to match that in this book.
- Test your service load and ensure that only services required for necessary functionality are running and enabled.
- Give strong passwords to service accounts.
- Never let users log on using service accounts.
- Do not allow network access to service accounts.
- Use accounts of least privilege for service accounts.
- Use the Microsoft Baseline Security Analyzer (MBSA) to analyze the current update level of machines on your network.
- Also visit Windows Update to identify and install appropriate hotfixes and software updates.
- Visit a reputable online software vendor and perform penetration tests on your machines to ensure that ports are closed off and your hardening efforts were effective.
- Format the partitions on your machines with NTFS.
- Disable automated logins by ensuring there is a password for each user account on a machine. (This applies only to machines that aren't participating in a security domain.)

- Rename the Administrator account.
- Rename the Guest account.
- Replace the Everyone group with the Authenticated Users group inside the access control lists (ACLs) of your shares.
- Use an account of least privilege for normal administrative work, and use Runas when you need an administrator security context.
- Disable infrared transfers.
- Understand the typical signs of a compromised machine.
- If a machine becomes compromised, don’t attempt to resurrect it. Get personal data off, verify the integrity of that data, and then reformat and reinstall the machine.