LESSON 5 : Protecting the Server and Client

OBJECTIVE DOMAIN MATRIX

SKILLS/CONCEPTS	MTA EXAM OBJECTIVE	MTA EXAM OBJECTIVE NUMBER
Protecting the Client Computer	Understand client protection.	4.1
Protecting Your Computer from Malware	Understand malware.	2.6
Protecting Your Email	Understand email protection.	4.2
Protecting Your Server	Understand server protection.	4.3
Securing Internet Explorer	Understand Internet security.	1.3

KEY TERMS

Adware

backdoor

Bayesian filter

content zones

cookie

malicious software (malware)

Microsoft Baseline Security Analyzer (MBSA)

offline files

pharming
phishing
pop-up window
rootkit

Sender Policy Framework (SPF)

spam

spyware

Trojan horse

User Account Control (UAC)

virus

virus hoax

Windows Defender

Windows Firewall

Windows Server Update Server

(WSUS)
Windows updates
worm

Say that you are talking to your company's CIO about your network security. In particular, you are trying to explain to him that you have established a multilayer approach to security. You have firewalls and other devices protecting the network borders to your organization. You also have protection configured for the servers and the clients. This way, if a hacker bypasses the external security layer, he or she will need to break through another layer to get to the network resources and confidential information.

Protecting the Client Computer

THE BOTTOM LINE
Users utilize client computers to connect to servers and network applications. Because these client computers are connected to an organization's network, they must be protected.

If you have been working with computers for much time, you know that protecting a client computer can be quite complicated. Most of these computers will run a Windows operating system, and even within a single organization, you will have a wide range of software applications and network services. Since the computer is how users usually connect to an organization's network, it is important that the client computers are kept secure from malware and intrusion.

CERTIFICATION READY
What does it take to secure a client computer?
4.1

Protecting Your Computer from Malware

Malicious software, sometimes called malware, is software that is designed to infiltrate or affect a computer system without the owner's informed consent. The term "malware" is usually associated with viruses, worms, Trojan horses, spyware, rootkits, and dishonest adware. As a network administrator or computer technician, you need to know how to identify malware, how to remove it, and how to protect a computer from it.

CERTIFICATION READY
Do you know how a buffer overflow is exploited?
2.6

LOOKING AT TYPES OF MALWARE

Because it is now quite common for computers to be connected to the Internet, there are more opportunities than ever before for your organization's computers to be infected by malware. Indeed, over the last few years, a staggering amount of malware has been produced. As a security professional, you are responsible for protecting your organization's computers against infection. Furthermore, if a computer on your network does somehow happen to get infected by malware, you must make sure this infection does not spread to other computers.

Many early forms of malware were written as experiments or pranks. Most of the time, they were intended to be harmless or merely annoying. However, as time passed, malware increasingly became a tool for vandalism or compromising private information. Today, malware can even be used to launch denial of service (DoS) attacks against other systems, networks, or websites, causing those systems to have performance problems or become inaccessible.

As mentioned before, malware can be divided into several categories, including the following:

- Viruses

- Worms
- Trojan horses
- Spyware and dishonest adware
- Rootkits
- Backdoors

A computer ***virus*** is a program that can copy itself and infect a computer without the user's consent or knowledge. Early viruses were usually some form of executable code that was hidden in the boot sector of a disk or as an executable file (e.g., a filename with a .exe or .com extension). Later, as macro languages began to be used in software applications (such as word processors and spreadsheet programs), virus creators seized upon this technology, embedding malicious macros in documents of various types. Unfortunately, because macro code is automatically executed when a document is opened, these documents can infect other files and cause a wide range of problems on affected computer systems. Today, websites also pose a virus threat, as they can be written in various programming and scripting languages and may include executable programs. Therefore, whenever you access the Internet, your system is under constant threat of infection.

A ***worm*** is a self-replicating program that copies itself to other computers on a network without any user intervention. Unlike a virus, a worm does not corrupt or modify files on the target computer. Instead, it consumes bandwidth and processor and memory resources, slowing the system down or causing it to be unusable. Worms usually spread via security holes in operating systems or TCP/IP software implementations.

Trojan horses derive their name from the Trojan horse story in Greek mythology. In short, a ***Trojan horse*** is an executable program that appears as a desirable or useful program. Because it appears to be desirable or useful, users are tricked into loading and executing the program on their systems. After the program is loaded, it might cause a user's computer to become unusable, or it might bypass the user's system security, allowing his or her private information (including passwords, credit card numbers, and Social Security number) to be accessible by an outside party. In some cases, a Trojan horse may even execute adware.

Spyware is a type of malware that is installed on a computer to collect a user's personal information or details about his or her browsing habits, often without the user's knowledge. Spyware can also install additional software, redirect your web browser to other sites, or change your home page. One example of spyware is the keylogger, which records every key a user presses. When a keylogger is installed on your system, whenever you type in credit card numbers, Social Security numbers, or passwords, that information is recorded and eventually sent to or read by someone without your knowledge. (It should be noted that not all keyloggers are bad, however, as some corporations use them to monitor their corporate users.)

Adware is any software package that automatically plays, displays, or downloads advertisements to a computer after the software is installed or while the application is being used. Although adware may not necessarily be bad, it is often used with ill intent.

A ***rootkit*** is a software or hardware device designed to gain administrator-level control over a computer system without being detected. Rootkits can target the BIOS, hypervisor, boot loader, kernel, or less commonly, libraries or applications.

A ***backdoor*** is a program that gives someone remote, unauthorized control of a system or initiates an unauthorized task. Some backdoors are installed by viruses or other forms of malware. Other backdoors may be created by programs on commercial applications or with a customized application made for an organization.

Viruses and worms often exploit what is known as a buffer overflow. In all application programs including Windows itself, there are buffers that hold data. These buffers have a fixed size. If too much data is sent to these buffers, a buffer overflow occurs. Depending on the data sent to the overflow, a hacker may be able to use the overflow to send passwords to himself or herself, alter system files, install backdoors, or cause errors on a computer. When patches are released to fix a potential buffer overflow, the patch adds code to check the length of data sent to the buffer to make sure that it does not overflow.

IDENTIFYING MALWARE

The first step in removing malware is detecting that you have it. Sometimes, it is easy to see that you are infected with malware. Other times, you may never know that you have it. Some common symptoms of malware include the following:

- Poor system performance
- Unusually low levels of available memory
- Poor performance while connected to the Internet
- Decreased response rates
- Longer start-up times
- Instances in which your browser closes unexpectedly or stops responding
- Changes in your browser’s default home or default search pages
- Unexpected pop-up advertising windows
- Addition of unexpected toolbars to your browser
- Instances in which unexpected programs automatically start
- Inability to start a program
- Malfunctions in Windows components or other programs
- Missing programs or files
- Unusual messages or displays on your monitor
- Unusual sounds or music played at random times
- Creation and/or installation of unknown programs or files
- Appearance of unknown browser add-ins

- Corrupted files
- Unexpected changes in file sizes

Of course, to see these symptoms, you may need to actively look for them. For example, when your Windows machine becomes slow, you might start Task Manager to view processor and memory utilization. You could then look at the ongoing processes to see which process is using the greatest amount of processor and memory resources. You might also review the processes and services in memory (again, you can use Task Manager). In addition, you could use the System Configuration. Of course, to be able to determine which processes and services are rogue, you need to have a baseline of what processes and services are currently running on your healthy system for comparison purposes. Finally, to detect malware, you should use an up-to-date antivirus program and an up-to-date antispyware package, which together can scan your entire system and look for malware in real time as you open files and access websites.

With the many tools attackers can now use to deliver malware, it is easy to see the importance of protecting your computer from all types of malware threats. Of course, when protecting yourself, a little common sense can go a long way.

USING SECURITY UPDATES AND ANTIVIRUS SOFTWARE FOR CLIENTS

Some viruses, worms, rootkits, spyware, and adware gain access to a system by exploiting security holes in Windows, Internet Explorer, Microsoft Office, or some other software package. Therefore, the first step you should take to protect yourself against malware is to keep your system up to date with the latest service packs, security patches, and other critical fixes.

The second step in protecting your computer from malware is to use an up-to-date antivirus software package. In addition, if your antivirus software does not include an antispyware component, you should install an antispyware software package. Then, you should be sure to perform a full system scan with your antivirus software at least once a week.

Windows Defender is a software product from Microsoft that is intended to prevent, remove, and quarantine spyware in Microsoft Windows. This program will help protect your computer against pop-ups, slow performance, and security threats caused by spyware and other unwanted software by detecting and removing known spyware from your computer. Windows Defender features real-time protection, a monitoring system that recommends actions against spyware as soon as it’s detected, and minimal interruptions to help you stay productive. Of course, as with any antivirus package, you must keep Windows Defender up to date.

DOWNLOAD
For Windows XP, Windows Defender can be downloaded from the following website:
http://www.microsoft.com/windows/products/winfamily/defender/default.mspx

USING COMMON SENSE WITH MALWARE

To avoid malware, it’s also important to use common sense. Therefore, you should always follow these steps:

1. Don’t install unknown software or software from an unreputable source.

2. Don’t open strange email attachments.

3. Don’t click on hyperlinks from unknown people when you don’t know what the links are supposed to do. This applies not just to hyperlinks sent via email, but also hyperlinks sent using instant messaging services.

4. If your email client supports auto launch, turn it off. Otherwise, you might automatically activate a computer virus just by opening an email.

5. Don’t visit questionable websites, especially porn sites or sites that allow you to download pirated software, music, or video.

6. If your web browser alerts you that a particular site is known for hosting malware, pay attention to this warning.

7. When surfing the Internet, if you encounter browser pop-ups that tell you that you need to download the newest driver or check your system for viruses, proceed with caution.

8. Don’t forget to perform regular backups. That way, if you get a virus and lose any data, you can restore your system from your backup.

TAKE NOTE*
Although this list may be common knowledge for IT personnel, all users should receive frequent reminders and awareness training to help protect your network.

REMOVING MALWARE

Whenever you start seeing any of the symptoms listed earlier in this lesson, you should quickly move to detect and (if necessary) remove any malware present on your system. Again, the first step in removing malware is to run an antivirus software package and perform a full scan. If you don’t already have antivirus software, this is a good time to purchase it. If you cannot download this software with your computer, try downloading it on another machine, then copying it to an optical disk (such as a CD or DVD) or a thumb drive to transfer it to your system. If the software finds malware and removes it, you should reboot your computer and run the program yet again to be sure your system is clean. If the program keeps finding different malware after reboot, you should continue repeating the process until your machine is clean.

Microsoft offers Microsoft Security Essentials (MSE), a free antivirus software product that provides protection from malware including viruses, rootkits, spyware, and Trojan horses. To download MSE, visit the following website:

http://www.microsoft.com/security_essentials/

TAKE NOTE*
Be sure that your antivirus software is up to date. If it is not current, it will not be able to detect newer viruses.

If your antivirus software package keeps finding the same malware over and over again, you need to be sure that you're not accessing a disk or other device that keeps infecting your system. You may also need to reboot Windows in safe mode and try another scan. If you have the option to do so, you can also try booting from a CD or DVD and running the scan.

If your software can't remove a particular virus, do a little research on the Internet. Often, you can find step-by-step instructions for removing malware, including deleting files and keys in the registry. Of course, be sure that the instructions are from a reliable source and that you follow them precisely.

Remember, if your antivirus package does not have an antispyware component, you should install a separate antispyware package to check for spyware. You can also use Windows Defender.

TAKE NOTE*
If you've purchased an antivirus software package and are having trouble removing malware, don't be afraid to contact the software company for assistance.

Microsoft also offers the Microsoft Windows Malicious Software Removal Tool, which checks computers running Windows for infections by specific, prevalent malware. Microsoft releases an updated version of this tool on the second Tuesday of each month, and as needed to respond to security incidents. The tool is available from Microsoft Update, Windows Update, and the Microsoft Download Center.

Finally, don't forget to use the following tools when trying to remove unknown malware:

- Use Task Manager to view and stop unknown processes and to stop unknown or questionable services.
- Use the Services MMC to stop unknown or questionable services.

TAKE NOTE*
Because some malware has keylogging capabilities, you may want to update your login information for your online accounts whenever you find and remove any malware.

- Use System Configuration to disable unknown or questionable services and startup programs.
- In Internet Explorer, be sure to disable any unknown or questionable add-ins.

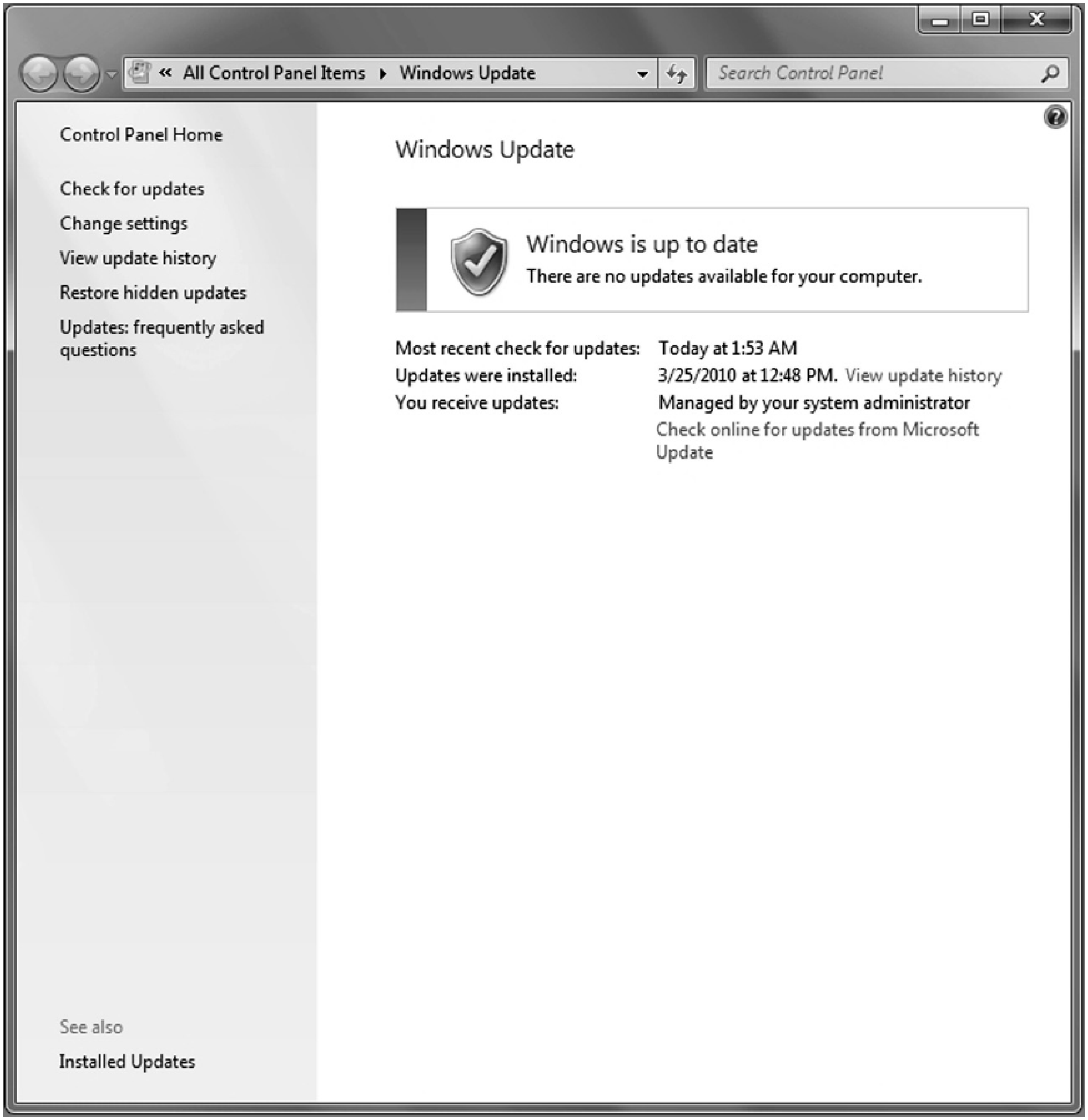
EXAMINING A VIRUS HOAX

A ***virus hoax*** is a message warning the recipient of a nonexistent computer virus threat, usually sent as a chain email that tells the recipient to forward it to everyone he or she knows. This is a form of social engineering that plays on people's ignorance and fear. Some hoaxes may tell people to delete key system files that make their system work properly. Others may advise you to download software from the Internet to protect against the supposed virus, when in reality, the downloaded software is some form of malware. Antivirus specialists agree that recipients should always delete virus hoaxes when they receive them, instead of forwarding them.

Utilizing Windows Updates

> After installing Windows, you should check to see whether Microsoft has released any ***Windows updates***, including fixes, patches, service packs, and updated device drivers. If so, you should apply them to your Windows system. By adding fixes and patches, you'll keep Windows stable and secure. Be aware that in some instances, Microsoft will release several fixes or patches together in the form of a service pack or cumulative package.

One way to keep Windows up to date is to use the Windows Update program. This program scans your system to determine what updates and fixes your system needs. You then have the opportunity to select, download, and install each update. See Figure 5-1.



Windows Update

Windows is up to date

There are no updates available for your computer.

Most recent check for updates: Today at 1:53 AM

Updates were installed: 3/25/2010 at 12:48 PM. View update history

You receive updates: Managed by your system administrator

Check online for updates from Microsoft Update

Figure 5-1 Windows Update

For corporations, you can also use ***Windows Server Update Service (WSUS)*** or System Center Configuration Manager (SCCM) to keep your systems updated. The advantage of using one of these two systems is that it allows you to test the patch, schedule the updates, and prioritize client updates. Once you determine a patch is safe, you can enable it for deployment.

Microsoft routinely releases security updates on the second Tuesday of each month, commonly known as “Patch Tuesday.” Most other updates are released as needed; these are known as “out of band” updates. Because computers are often used as production systems, you should test any updates to make sure they do not cause problems for you. Although Microsoft performs intensive testing, occasionally problems do occur, either as a bug or as a compatibility issue with third-party software. Therefore, always be sure you have a good backup of your system and data files before you install patches so that you have a back-out plan if necessary.

Microsoft classifies updates as Important, Recommended, or Optional:

- **Important updates:** These updates offer significant benefits, such as improved security, privacy, and reliability. They should be installed as they become available and can be installed automatically with Windows Update.
- **Recommended updates:** These updates address noncritical problems or help enhance your computing experience. Although these updates do not address fundamental issues with your computer or Windows software, they can offer meaningful improvements.
- **Optional updates:** These include updates, drivers, or new software from Microsoft to enhance your computing experience. You need to install these manually.

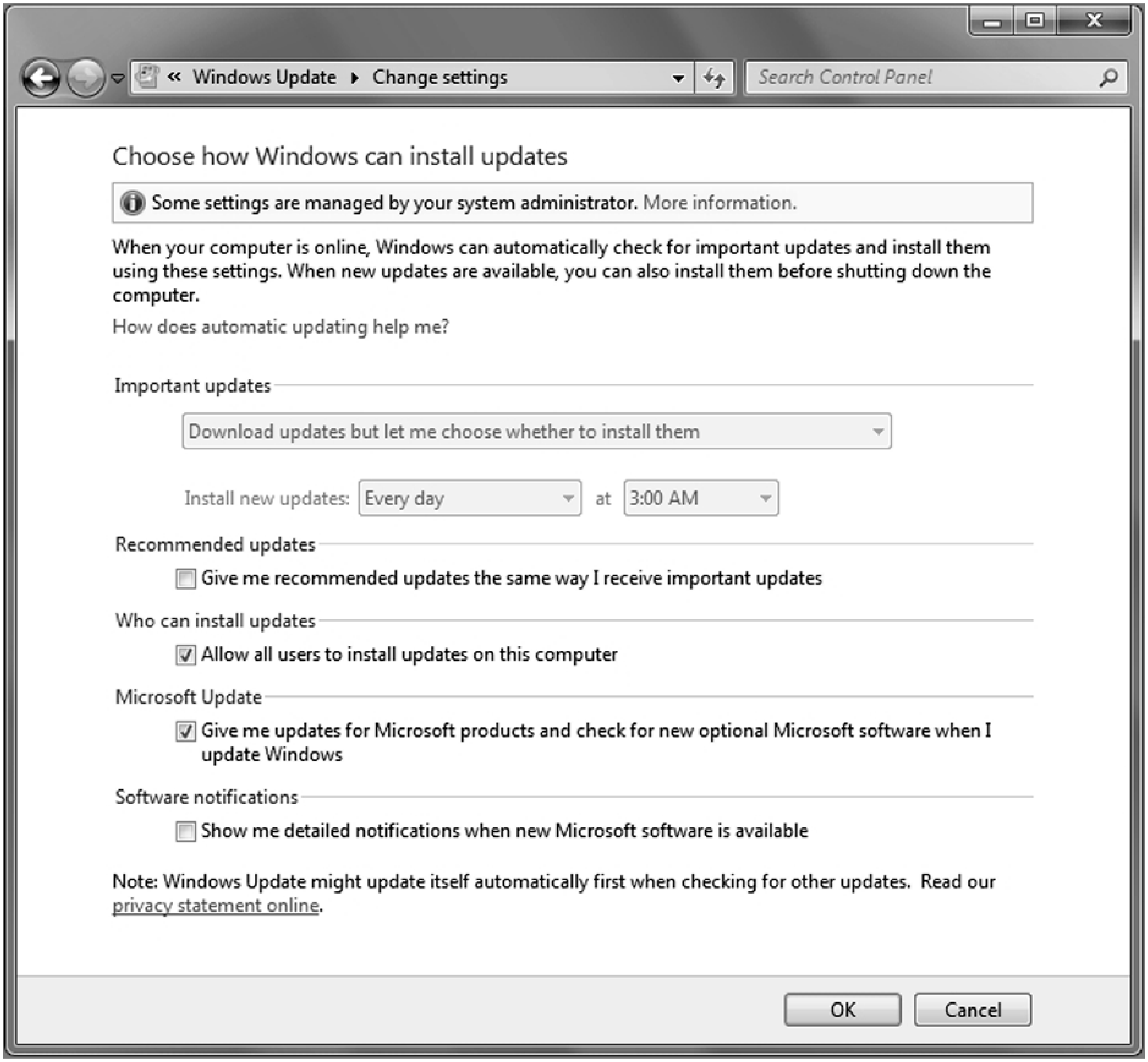
Depending on the type of update, Windows Update can deliver the following:

- **Security updates:** A security update is a broadly released fix for a product-specific security-related vulnerability. Security vulnerabilities are rated based on their severity, which is indicated in the Microsoft security bulletin as critical, important, moderate, or low.
- **Critical updates:** A critical update is a broadly released fix for a specific problem addressing a critical, nonsecurity related bug.
- **Service packs:** A service pack is a tested, cumulative set of hotfixes, security updates, critical updates, and updates, as well as additional fixes for problems found internally since the release of the product. Service packs might also contain a limited number of customer-requested design changes or features. After an operating system is released, many corporations consider the first service pack as the time when the operating system has matured enough to be used throughout the organization.

Not all updates can be retrieved through Windows Update. Sometimes, Microsoft may offer the fix for a specific problem in the form of a hotfix or cumulative patch that you can install. A hotfix is a single, cumulative package that includes one or more files that are used to address a problem in a software product, such as a software bug. Typically, hotfixes are made to address a specific customer situation, and they often have not gone through the same extensive testing as patches retrieved through Windows Updates.

For small environments, you can configure your system to run Auto Update to ensure that critical, security, and compatibility updates are made available for installation automatically without significantly affecting your regular use of the Internet. Auto Update works in the background when you are connected to the Internet to identify when new updates are available and to download them to your computer. When a download is complete, you are notified and prompted to install the update. At this point, you can install the update, get more details about what is included in the update, or let Windows remind you about the update at a later time. Some updates require you to reboot, but some do not.

To change your Windows Update settings, click the Change settings option in the left pane of the Windows Update window. See Figure 5-2. Here, you can specify which types of updates you want to download and install automatically, or you can disable Windows Update all together. You can also specify whether Windows Update will check for updates for other Microsoft products and/or install any other software Microsoft recommends.



Choose how Windows can install updates

Some settings are managed by your system administrator. More information.

When your computer is online, Windows can automatically check for important updates and install them using these settings. When new updates are available, you can also install them before shutting down the computer.

How does automatic updating help me?

Important updates

Download updates but let me choose whether to install them

Install new updates: Every day at 3:00 AM

Recommended updates

□ Give me recommended updates the same way I receive important updates

Who can install updates

☑ Allow all users to install updates on this computer

Microsoft Update

☑ Give me updates for Microsoft products and check for new optional Microsoft software when I update Windows

Software notifications

□ Show me detailed notifications when new Microsoft software is available

Note: Windows Update might update itself automatically first when checking for other updates. Read our privacy statement online.

Figure 5-2 Changing Windows Update settings

If Windows Update fails to retrieve any updates, you should check your proxy settings in Internet Explorer to see whether the program can get through your proxy server (if any) or firewall. You should also check to see whether you can access the Internet, such as by going to **http://www.microsoft.com.**

To see all updates that have been installed, click View Update History on the main screen of Windows Update. If you suspect a problem with a specific update, you can then click Installed Updates at the top of the screen to open the Control Panel’s programs. From there, you will see all installed programs and updates. If the option is available, you can then remove the update.

Utilizing User Account Control

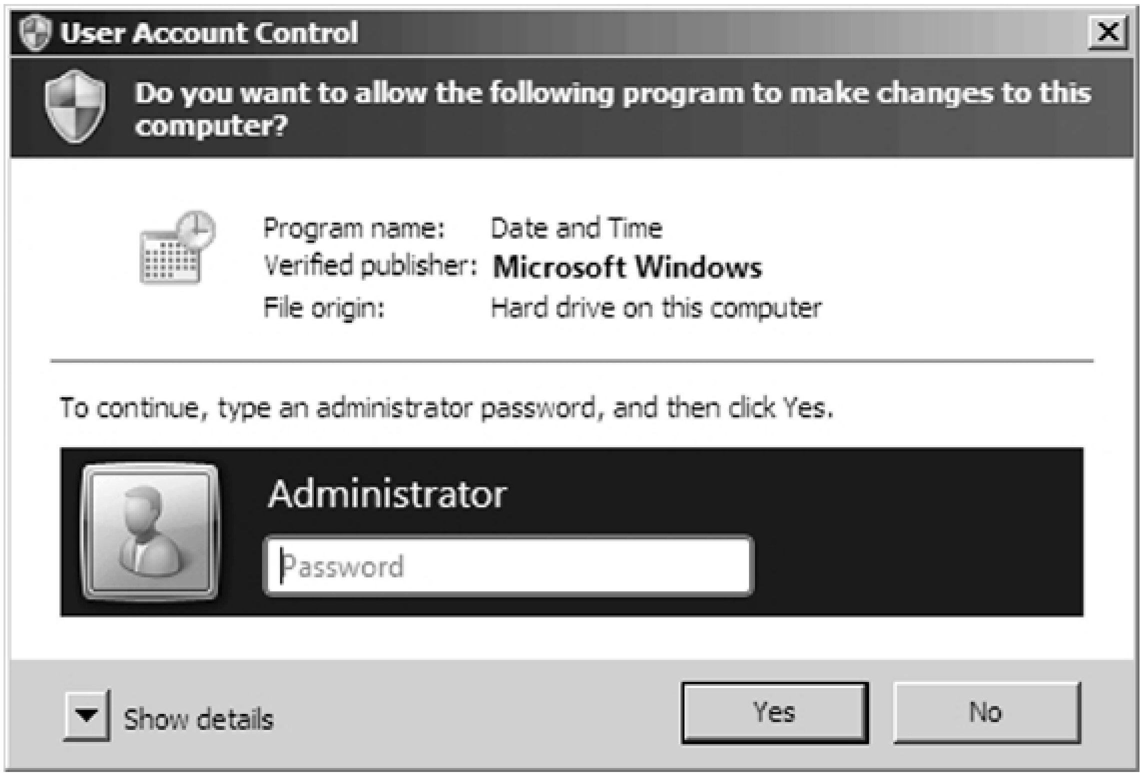
User Account Control (UAC) is a feature that started with Windows Vista and is included with Windows 7. UAC helps prevent unauthorized changes to your computer—and in doing so, it helps protect your system from malware.

If you are logged in as an administrator, UAC asks you for permission before performing actions that could potentially affect your computer's operation or change settings that affect other users. Similarly, if you are logged in as a standard user, UAC will ask you for an administrator password before taking such actions. Because UAC is designed to prevent unauthorized changes—especially those made by malicious software that you may not know you are running—you need to read these warnings carefully, making sure that the action or program that's about to start is one you intended to start.

As a standard user, in Windows 7, you can do the following without administrative permissions or rights:

- Install updates from Windows Update
- Install drivers from Windows Update or drivers that are included with the operating system
- View Windows settings
- Pair Bluetooth devices with a computer
- Reset the network adapter and perform other network diagnostic and repair tasks

When an application requests elevation or is run as an administrator, UAC will prompt for confirmation and, if consent is given, it will allow access as an administrator. See Figure 5-3.



User Account Control

Do you want to allow the following program to make changes to this computer?

Program name: Date and Time
Verified publisher: Microsoft Windows
File origin: Hard drive on this computer

To continue, type an administrator password, and then click Yes.

Administrator

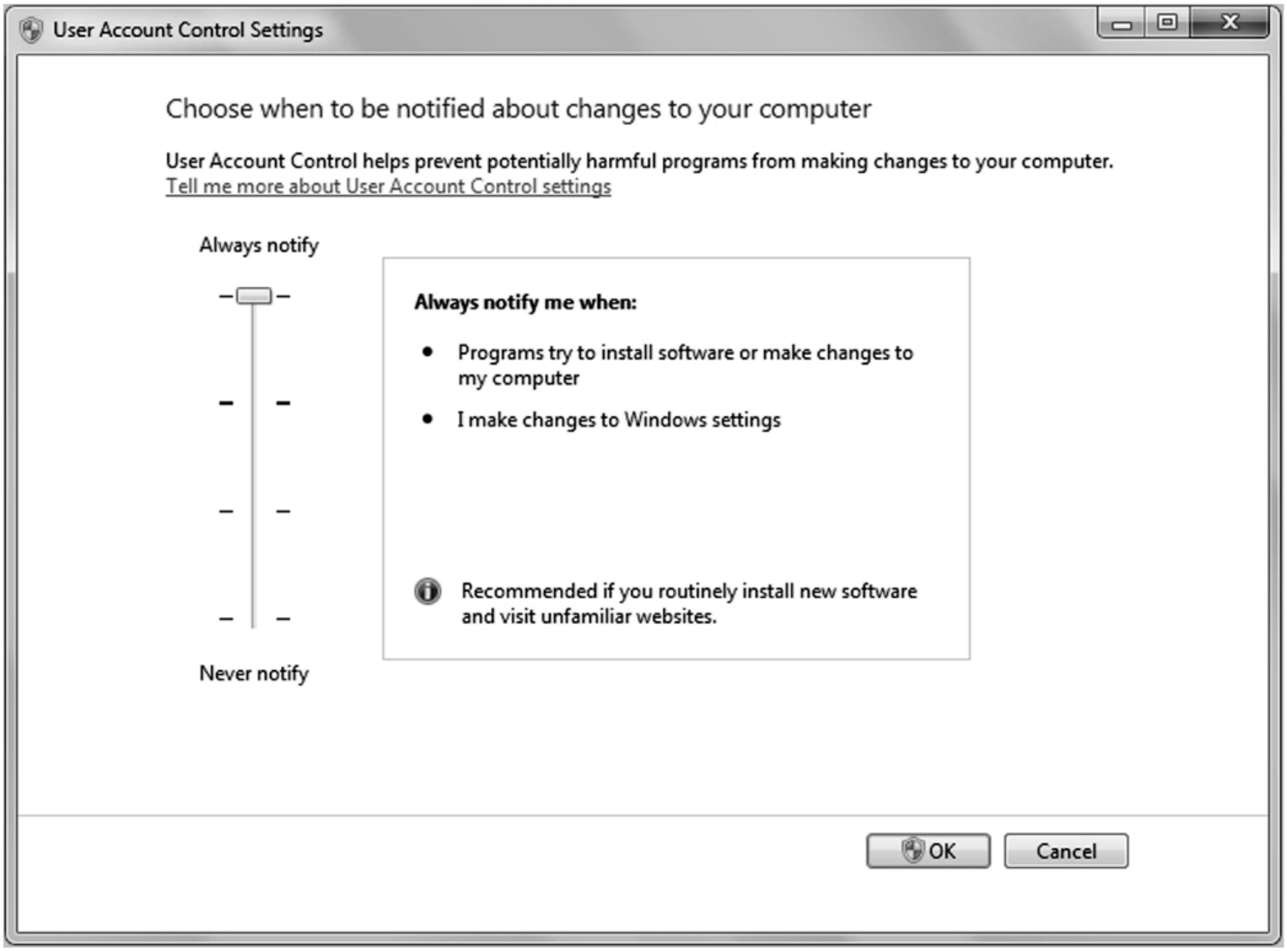
Figure 5-3 UAC confirmation with Secure Desktop

UAC can be enabled or disabled for any individual user account. Of course, if you disable UAC for a user account, your computer will be at greater risk. However, if you perform a lot of administrative tasks on a computer, repeated UAC prompts can be annoying and can stop you from doing certain activities, including saving to the root directory of a drive if you have an application that is not compatible with UAC.

ENABLE OR DISABLE UAC

GET READY. To enable or disable UAC, follow these steps:

1. In **Control Panel**, click **User Accounts**.
2. On the **User Accounts** page, click **User Accounts**.
3. Click the **Change User Account Control settings**.
4. Slide the slider to the desired options, as shown in Table 5-1. (See Figure 5-4.)



User Account Control Settings

Choose when to be notified about changes to your computer

User Account Control helps prevent potentially harmful programs from making changes to your computer.
Tell me more about User Account Control settings

Always notify

Never notify

Always notify me when:

- Programs try to install software or make changes to my computer
- I make changes to Windows settings

Recommended if you routinely install new software and visit unfamiliar websites.

Figure 5-4 UAC settings

5. When prompted to restart the computer, click **Restart Now** or **Restart Later** as appropriate for the changes to take effect.

Table 5-1 UAC settings

SETTING	DESCRIPTION	SECURITY IMPACT
Always notify	You will be notified before programs make changes to your computer or to Windows settings that require the permissions of an administrator. When you're notified, your desktop will be dimmed, and you must either approve or deny the request in the UAC dialog box before you can do anything else on your computer. The dimmed desktop is referred to as a secure desktop because other programs can't run while it's dimmed.	This is the most secure setting. When you are notified, you should carefully read the contents of each dialog box before allowing changes to be made to your computer.
Notify me only when programs try to make changes to my computer	You will be notified before programs make changes to your computer that require the permissions of an administrator. You will not be notified if you try to make changes to Windows settings that require the permissions of an administrator. You will be notified if a program outside of Windows tries to make changes to a Windows setting.	It's usually safe to allow changes to be made to Windows settings without notification. However, certain programs that come with Windows can have commands or data passed to them, and malicious software can take advantage of this by using these programs to install files or change settings on your computer. You should always be careful about which programs you allow to run on your computer.
Notify me only when programs try to make changes to my computer (do not dim my desktop)	You will be notified before programs make changes to your computer that require the permissions of an administrator. You will not be notified if you try to make changes to Windows settings that require the permissions of an administrator. You will be notified if a program outside of Windows tries to make changes to a Windows setting.	This setting is the same as "Notify only when programs try to make changes to my computer," but you are not notified on the secure desktop. Because the UAC dialog box isn't on the secure desktop with this setting, other programs might be able to interfere with the dialog's visual appearance. This is a small security risk if you already have a malicious program running on your computer.

SETTING	DESCRIPTION	SECURITY IMPACT
Never notify	You will not be notified before any changes are made to your computer. If you are logged on as an administrator, programs can make changes to your computer without you knowing about it. If you are logged on as a standard user, any changes that require the permissions of an administrator will automatically be denied. If you select this setting, you will need to restart the computer to complete the process of turning off UAC. Once UAC is off, people who log on as an administrator will always have the permissions of an administrator.	This is the least secure setting. When you set UAC to never notify, you open up your computer to potential security risks. If you set UAC to never notify, you should be careful about which programs you run, because they will have the same access to the computer as you do. This includes reading and making changes to protected system areas, personal data, saved files, and anything else stored on the computer. Programs will also be able to communicate and transfer information to and from anything your computer connects with, including the Internet.

Using Windows Firewall

Another important client tool is a firewall. As discussed in Lesson 4, a firewall is software or hardware that checks information coming from the Internet or a network, and then either blocks it or allows it to pass through to your computer, depending on your firewall settings. A firewall can help prevent hackers or malicious software (such as worms) from gaining access to your computer through a network or the Internet. A firewall can also help stop your computer from sending malicious software to other computers.

Microsoft recommends that you always use ***Windows Firewall***. However, because some security packages and antivirus packages include their own firewall, you may choose to run an alternate firewall—but you should use only one firewall.

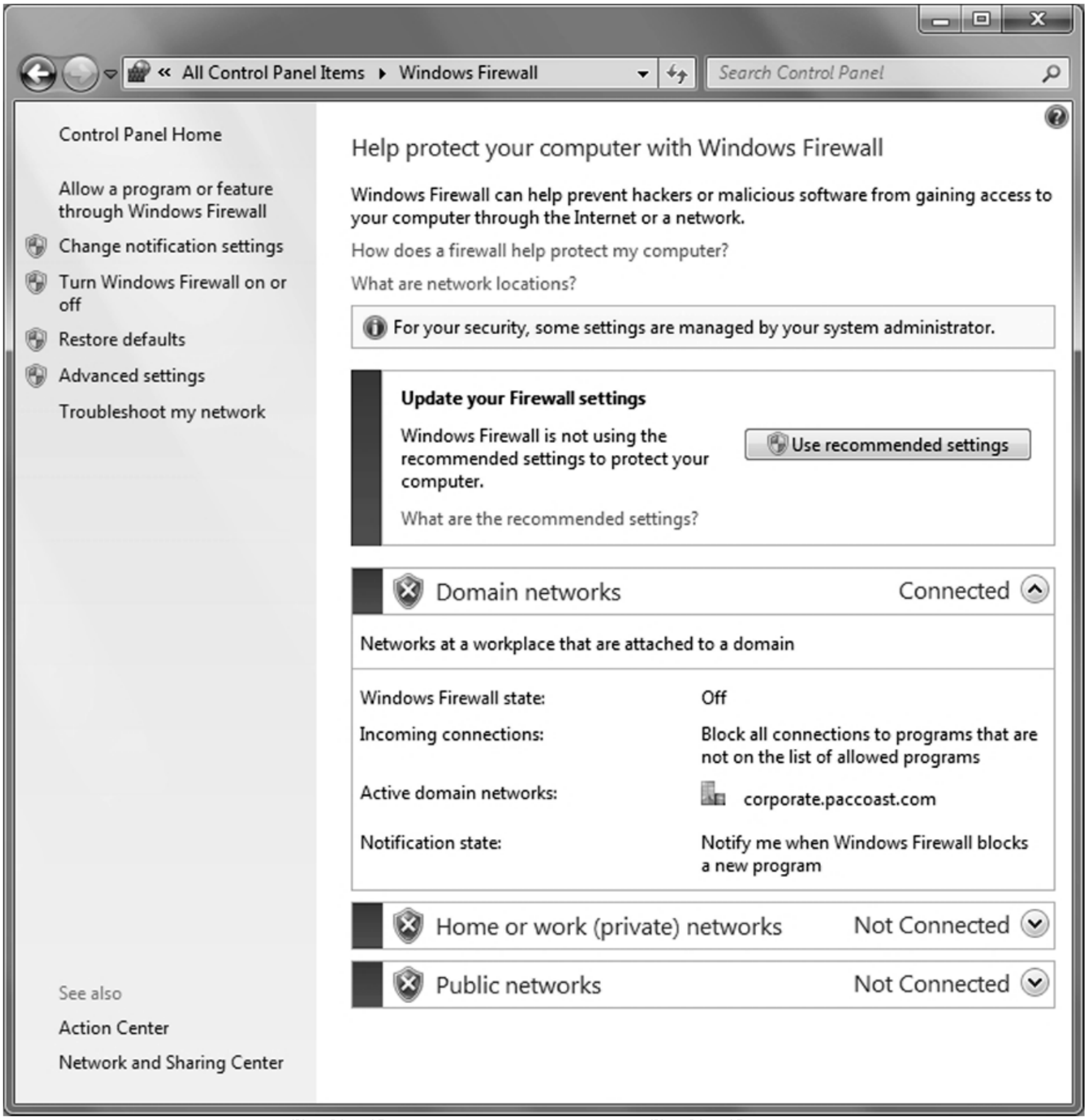
TAKE NOTE*
Although your network may have a firewall to help protect you from unwanted Internet traffic, it's still a good idea to have a host firewall to give you an extra level of protection. This is especially recommended when the client computer is a mobile computer that may be moved outside your organization's network.

In addition, to the Windows Firewall found in the Control Panel, newer versions of Windows include Windows Firewall with Advanced Security. Windows Firewall with Advanced Security combines a host firewall and Internet Protocol security (IPsec). Although Windows Firewall and Windows Firewall with Advanced Security are tightly coupled, the latter allows greater control of your firewall. In addition, Windows Firewall with Advanced Security also provides computer-to-computer connection security by allowing you to require authentication and data protection for communications via IPsec.

ENABLE OR DISABLE WINDOWS FIREWALL

GET READY. To enable or disable Windows Firewall, perform the following steps:

1. Open the **Control Panel**.
2. If you are in **Category** view, click **System and Security**, then click **Windows Firewall**. If you are in **Icon** view, double-click **Windows Firewall**.
3. In the left pane, click **Turn Windows Firewall on or off**. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.
4. Click **Turn on Windows Firewall** under the appropriate network location to enable Windows Firewall, or click **Turn off Windows Firewall (not recommended)** under the appropriate network location to disable Windows Firewall. See Figure 5-5. You typically want to block all incoming traffic when you connect to a public network in a hotel or airport or when a computer worm is spreading over the Internet. When you block all incoming connections, you can still view most web pages, send and receive email, and send and receive instant messages.



« All Control Panel Items ▸ Windows Firewall
Search Control Panel
Control Panel Home
Allow a program or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Action Center
Network and Sharing Center
Use recommended settings

Help protect your computer with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.

How does a firewall help protect my computer?

What are network locations?

For your security, some settings are managed by your system administrator.

Update your Firewall settings

Windows Firewall is not using the recommended settings to protect your computer.

What are the recommended settings?

Domain networks — Connected

Networks at a workplace that are attached to a domain

Windows Firewall state:	Off
Incoming connections:	Block all connections to programs that are not on the list of allowed programs
Active domain networks:	corporate.paccoast.com
Notification state:	Notify me when Windows Firewall blocks a new program

Home or work (private) networks — Not Connected

Public networks — Not Connected

Figure 5-5 Windows Firewall

5. If desired, select **Block all incoming connections, including those in the list of allowed programs** and **Notify me when Windows Firewall blocks a new program**.

6. Click **OK**.

By default, most programs are blocked by Windows Firewall to help make your computer more secure. To work properly, some programs might require you to allow them to communicate through the firewall.

ALLOW A PROGRAM THROUGH WINDOWS FIREWALL

GET READY. To allow a program to communicate through Windows Firewall, perform the following steps:

1. Open **Windows Firewall**.

2. In the left pane, click **Allow a program or feature through Windows Firewall**.

3. Click **Change settings**. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.

4. Select the check box next to the program you want to allow, select the network locations you want to allow communication on, and then click **OK**.

OPEN PORTS ON WINDOWS FIREWALL

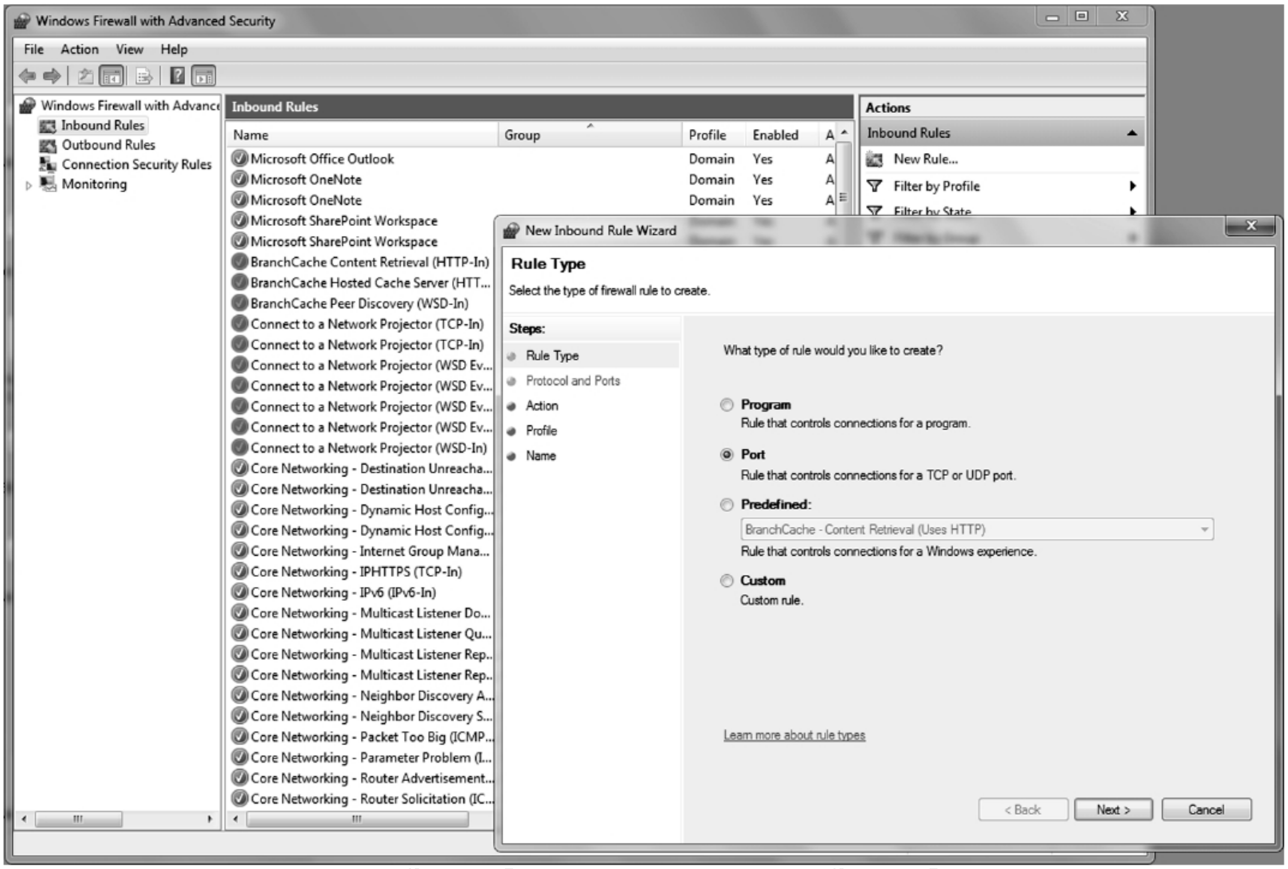
GET READY. If the program you want to allow isn't listed, you might need to open a port. To open a port, perform the following steps:

1. Open **Windows Firewall**.

2. In the left pane, click **Advanced settings**. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.

3. In the left pane of the **Windows Firewall with Advanced Security** dialog box, click **Inbound Rules**; then, in the right pane, click **New Rule**.

4. Select **Port** and click the **Next** button. See Figure 5-6.


Windows Firewall with Advanced Security
File Action View Help
Windows Firewall with Advance
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Inbound Rules
Name Group Profile Enabled A
Microsoft Office Outlook Domain Yes
Microsoft OneNote Domain Yes
Microsoft OneNote Domain Yes
Microsoft SharePoint Workspace
Microsoft SharePoint Workspace
BranchCache Content Retrieval (HTTP-In)
BranchCache Hosted Cache Server (HTT...
BranchCache Peer Discovery (WSD-In)
Connect to a Network Projector (TCP-In)
Connect to a Network Projector (TCP-In)
Connect to a Network Projector (WSD Ev...
Connect to a Network Projector (WSD Ev...
Connect to a Network Projector (WSD Ev...
Connect to a Network Projector (WSD Ev...
Connect to a Network Projector (WSD-In)
Core Networking - Destination Unreacha...
Core Networking - Destination Unreacha...
Core Networking - Dynamic Host Config...
Core Networking - Dynamic Host Config...
Core Networking - Internet Group Mana...
Core Networking - IPHTTPS (TCP-In)
Core Networking - IPv6 (IPv6-In)
Core Networking - Multicast Listener Do...
Core Networking - Multicast Listener Qu...
Core Networking - Multicast Listener Rep...
Core Networking - Multicast Listener Rep...
Core Networking - Neighbor Discovery A...
Core Networking - Neighbor Discovery S...
Core Networking - Packet Too Big (ICMP...
Core Networking - Parameter Problem (I...
Core Networking - Router Advertisement...
Core Networking - Router Solicitation (IC...
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
New Inbound Rule Wizard
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
Learn more about rule types
< Back
Next >
Cancel

Rule Type

Select the type of firewall rule to create.

What type of rule would you like to create?

○ **Program**
Rule that controls connections for a program.

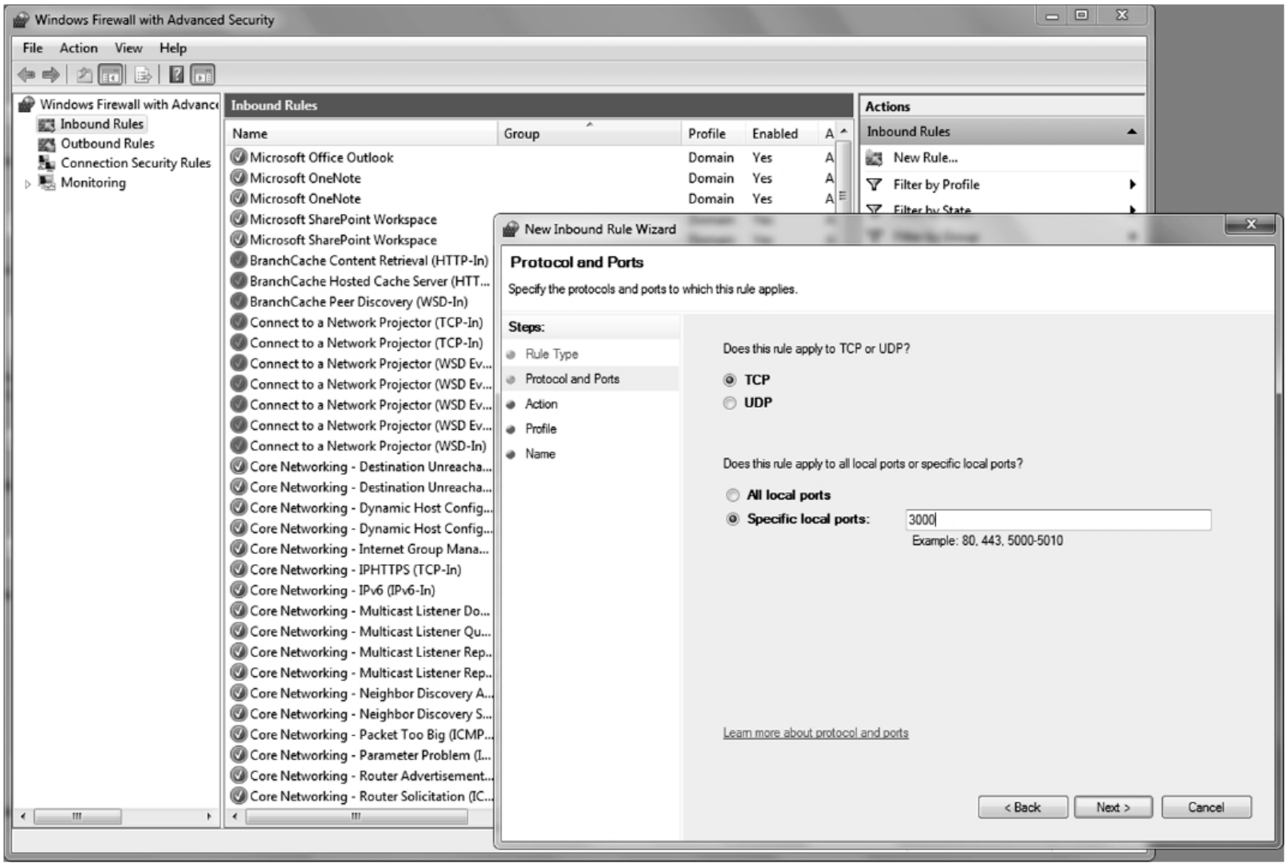
● **Port**
Rule that controls connections for a TCP or UDP port.

○ **Predefined:**
BranchCache - Content Retrieval (Uses HTTP)
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.

Figure 5-6 Inbound Rules options

5. Specify **TCP** or **UDP** and specify the port numbers. Click the **Next** button. See Figure 5-7.



Protocol and Ports

Specify the protocols and ports to which this rule applies.

Does this rule apply to TCP or UDP?

● **TCP**
○ **UDP**

Does this rule apply to all local ports or specific local ports?

○ **All local ports**
● **Specific local ports:** 3000
Example: 80, 443, 5000-5010

Figure 5-7 Opening a port

6. Select **Allow the connection**, **Allow the connection if it is secure**, or **Block the connection**. Click the **Next** button.

7. By default, the rule will apply to all domains. If you don't want the rule to apply to a domain, deselect the domain. Click the **Next** button.

8. Specify a name for the rule and a description if desired. Click the **Finish** button.

Using Offline Files

Offline files are copies of network files that are stored on your computer so you can access them when you aren't connected to the network or when the network folder that contains the files is not connected.

Offline files are not encrypted unless you choose for them to be. You might want to encrypt your offline files if they contain sensitive or confidential information and you want to make them more secure by restricting access to them. Encrypting your offline files provides you with an additional level of access protection that works independently of NTFS file system permissions. This can help safeguard your files in case your computer is ever lost or stolen.

ENABLE OFFLINE FILES

GET READY. To enable offline files, perform these steps:

1. Click the **Start** button and open the **Control Panel**.
2. Search for **offline** in the **Search Control Panel** text box and click **Manage offline files**.
3. Click **Enable offline files**.
4. If prompted, reboot the computer.

ENCRYPT OFFLINE FILES

GET READY. To encrypt your offline files, perform these steps:

1. Click the **Start** button and open the **Control Panel**.
2. Search for **offline** in the **Search Control Panel** text box and click **Manage offline files**.
3. Click the **Encryption** tab.
4. Click **Encrypt** to encrypt your offline files, and then click **OK**.

If you choose to encrypt your offline files, you encrypt only the offline files stored on your computer, not the network versions of the files. You do not need to decrypt an encrypted file or folder stored on your computer before using it. This is done for you automatically.

Locking Down a Client Computer

> If you work with end users for an extended period of time, you will soon learn that some users are their own worst enemy. Therefore, in some case, you should considering locking down a computer so that a user cannot harm it.

Unless individual users have the need to be administrators on their own computers, they should just be standard users. This will prevent users from installing unauthorized software and making changes to the system that would make the system less secure. In addition, if these users are affected by malware, the malware will only have minimum access to the system. Of course, it would be recommended to use the run as options if needed as discussed in Lesson 2.

When working within an organization, it is often advantageous to standardize each company computer. Therefore, when moving from one computer to another, everything will be similar. To keep computers standardized, an organization may choose to use Group Policies so that users cannot access certain features (including the Control Panel) and make changes to the system that may be detrimental.

Allowing users to install software may:

- Introduce malware to a system.
- Bypass safeguards already put in place to protect against malicious viruses and Trojan horse programs.
- Cause conflicts with software already on a baseline computer within an organization.

If you do not allow your computer users to log on as administrators, you limit what software they can install. You can also use group policies to restrict what software can be executed on a client computer.

Windows 7 supports two mechanisms for restricting applications both of which are based on group policies. They are:

- Software restriction policies
- AppLockerS

Protecting Your Email

> **THE BOTTOM LINE**

Email has become an essential service for virtually every corporation. Unfortunately, much of the email received by a company's employees consists of unsolicited messages called ***spam*** or junk email, some of which can carry malware and may lead to fraud or scams.

The idea behind spam is to send a lot of unsolicited bulk messages indiscriminately, hoping that a few people will open the email, navigate to a website, purchase a product, or fall for a scam. For the people who create it, spam has minimal operating costs. Over the last few years, spam amounts have increased exponentially, and today, spam accounts for at least 90 percent of all the email in the world.

CERTIFICATION READY
Do you know how to prevent viruses from being sent through email?
4.2

Besides the risk of malware and fraud associated with spam, there is also a loss of productivity for email recipients as they sort through unsolicited emails. In addition, the IT department will need to install additional storage and provide sufficient bandwidth to accommodate the extra email. Therefore, you should always install a spam blocking device or software that includes antivirus protection. The program will provide a second layer to protect your network from viruses.

Dealing with Spam

To keep your systems running smoothly, you—the network administrator—must put some effort into blocking spam.

The best place to establish a spam filtering system is on a dedicated server or appliance or as part of a firewall device or service. You can direct all email to the spam filter by changing your DNS Mail Exchanger (MX) record to point to the antispam server or device. Any email that is not considered spam will be forwarded to your internal email servers.

When establishing a spam filtering system, keep two things in mind. First, spam filtering systems will not catch every single spam message. Like an antivirus package, a spam filtering solution needs to be kept up to date and constantly tweaked. You may also need to add email addresses, email domains, IP address ranges, or keywords into a black list. Any email with traits on the black list will automatically be blocked. Of course, you need to take care when using a black list to make sure you don't make the criteria so broad as to start blocking legitimate email.

Many antispam solutions also use a real-time blackhole list (RBL) or DNS-based blackhole list (DNSBL) that can be accessed freely. RBLs and DNSBLs are lists of known spammers that are updated frequently. Most mail server software can be configured to reject or flag messages that have been sent from a site listed on one or more such lists. Because spammers look for ways to get around this, it is just one tool that can help reduce the amount of spam that gets through.

As email is identified as spam, it is usually quarantined or stored temporarily in case a legitimate email has been mistakenly placed in this category. While the number of miscategorized messages should be relatively low, you will need to train your help desk personnel and possibly your users to access quarantined email so they can release misplaced messages to their destined email box. In addition, you need to add the sender's email address or domain to a white list so that it will not be identified as spam in the future.

Detecting spam can be a daunting task if you've ever had to do it manually. Besides the obvious advertising phrases and other keywords, spam systems will also look at an email's header to analyze information about the email and its origin. For example, if you have email in Outlook 2003, open one email message, open the View menu, and select Options. Under Internet Headers, you can see the history for an email delivery path. To do this in Outlook 2010, first select the message, then click the File menu and select Properties under Info.

To make a spam message look like a legitimate message, sometimes spammers try to spoof an email address or IP address where a message comes from. For example, if email was sent from a yahoo.com domain, an antispam system could do a reverse lookup using the DNS PTR record to see the IP address of the yahoo.com domain. If that IP address does not match where the email said it came from, the message is considered spam and will be blocked.

Sender Policy Framework (SPF) is an email validation system designed to prevent email spam that uses source address spoofing. SPF allows administrators to specify in DNS SPF records in the public DNS which hosts are allowed to send email from a given domain. If email for a domain is not sent from a host listed in the DNS SPF, it will be considered spam and blocked.

Today, antispam packages use special algorithms, such as ***Bayesian filters***, to determine whether email is considered spam. These algorithms usually analyze previously received emails and create a database using a number of attributes. Then, when a computer receives an email, it will compare that email with the attributes it has collected to determine whether the message is spam.

Relaying Email

Simple Mail Transfer Protocol (SMTP) is one of the primary email protocols. SMTP is used to transfer email from one server to another, and it is responsible for outgoing mail transport. SMTP uses TCP port 25.

Although you may think your email servers function only for users to send and retrieve email, they also may be used to relay email. For example, web and application servers may relay email through their email servers, such as when you order something over the Internet and a confirmation email is sent to you.

Usually, you only want your internal servers to relay email through your mail servers.

Unfortunately, spammers frequently look for unprotected SMTP servers to relay their email through. As a result, not only do the spammers use your SMTP servers to send emails, but other organizations may flag your server or domain as a spammer, and you may be placed on one of the RBLs or DNSBLs. To get off this list, you will need to close up your security hole so that other people cannot relay email through your server. Then you can contact the organizations that host the RBLs or DNSBLs to get taken off their list.

Securing Internet Explorer

THE BOTTOM LINE
Because browsing a website can expose you to a wide range of hazards, you also need to look carefully at your browser to help protect both you and your system. Today's browsers include pop-up blockers, zones, and other built-in security features.

Looking at Cookies and Privacy Settings

CERTIFICATION READY
Where do you think most malware comes from?
1.3

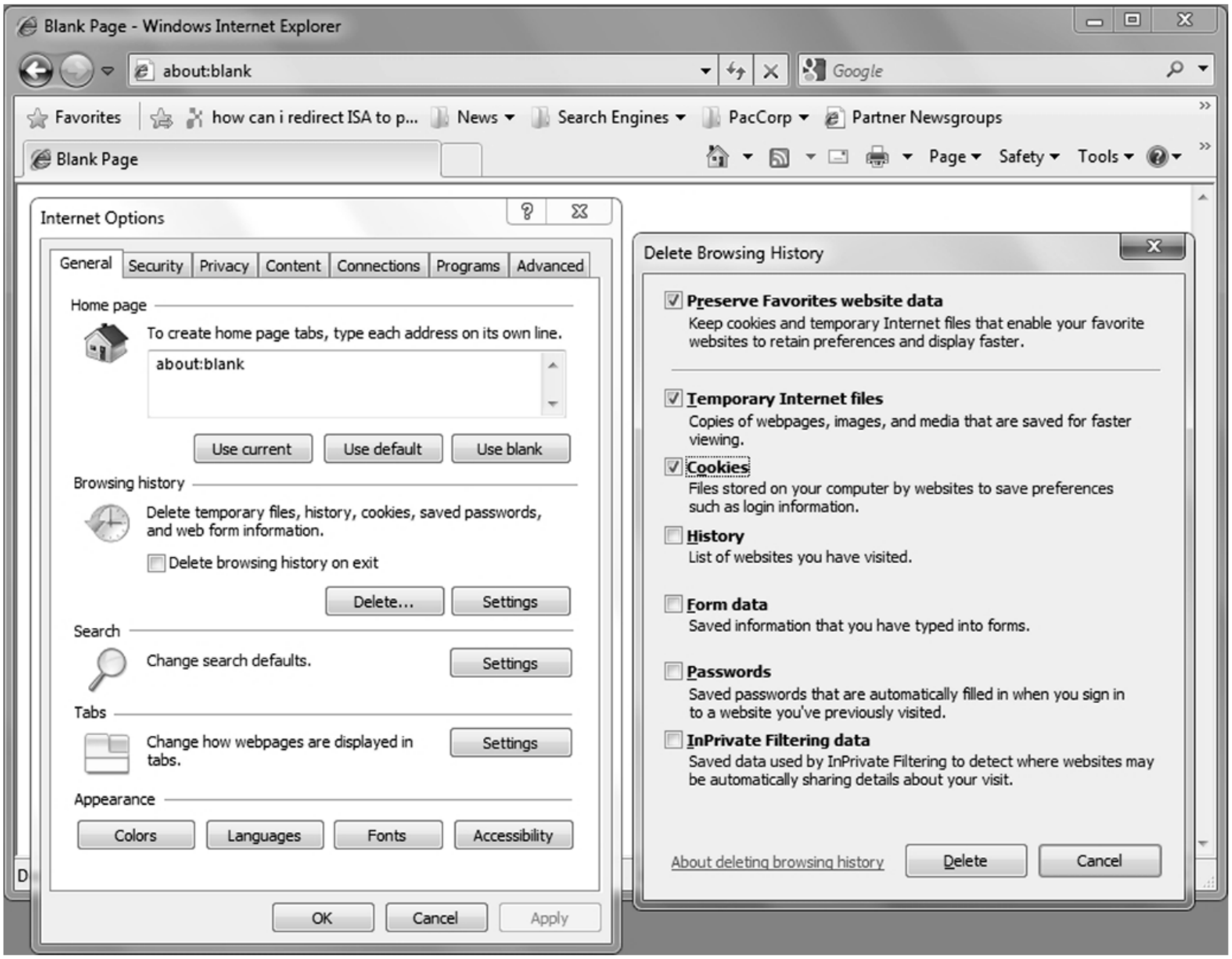
When you use a browser to access the Internet, you may be revealing personal information and a great deal about your personality. Therefore, you need to take steps to ensure that this information cannot be read or used without your knowledge.

A ***cookie*** is a piece of text stored by a user's web browser. This file can be used for a wide range of purposes, including user identification, authentication, and storing site preferences and shopping cart contents. Although cookies can give a website a lot of capability, they can also be used by spyware programs and websites to track people. Unfortunately, some websites will not operate without cookies.

DELETE COOKIES IN INTERNET EXPLORER 8

GET READY. To delete cookies, perform these steps:

1. Open **Internet Explorer**.
2. Click the **Tools** button, and then click **Internet Options**.
3. On the **General** tab, under **Browsing history**, click **Delete**. See Figure 5-8.



Home page

To create home page tabs, type each address on its own line.

about:blank

Browsing history

Delete temporary files, history, cookies, saved passwords, and web form information.

□ Delete browsing history on exit

Search

Change search defaults.

Tabs

Change how webpages are displayed in tabs.

Appearance

☑ **Preserve Favorites website data**
Keep cookies and temporary Internet files that enable your favorite websites to retain preferences and display faster.

☑ **Temporary Internet files**
Copies of webpages, images, and media that are saved for faster viewing.

☑ **Cookies**
Files stored on your computer by websites to save preferences such as login information.

□ **History**
List of websites you have visited.

□ **Form data**
Saved information that you have typed into forms.

□ **Passwords**
Saved passwords that are automatically filled in when you sign in to a website you've previously visited.

□ **InPrivate Filtering data**
Saved data used by InPrivate Filtering to detect where websites may be automatically sharing details about your visit.

Figure 5-8 Deleting cookies and temporary files

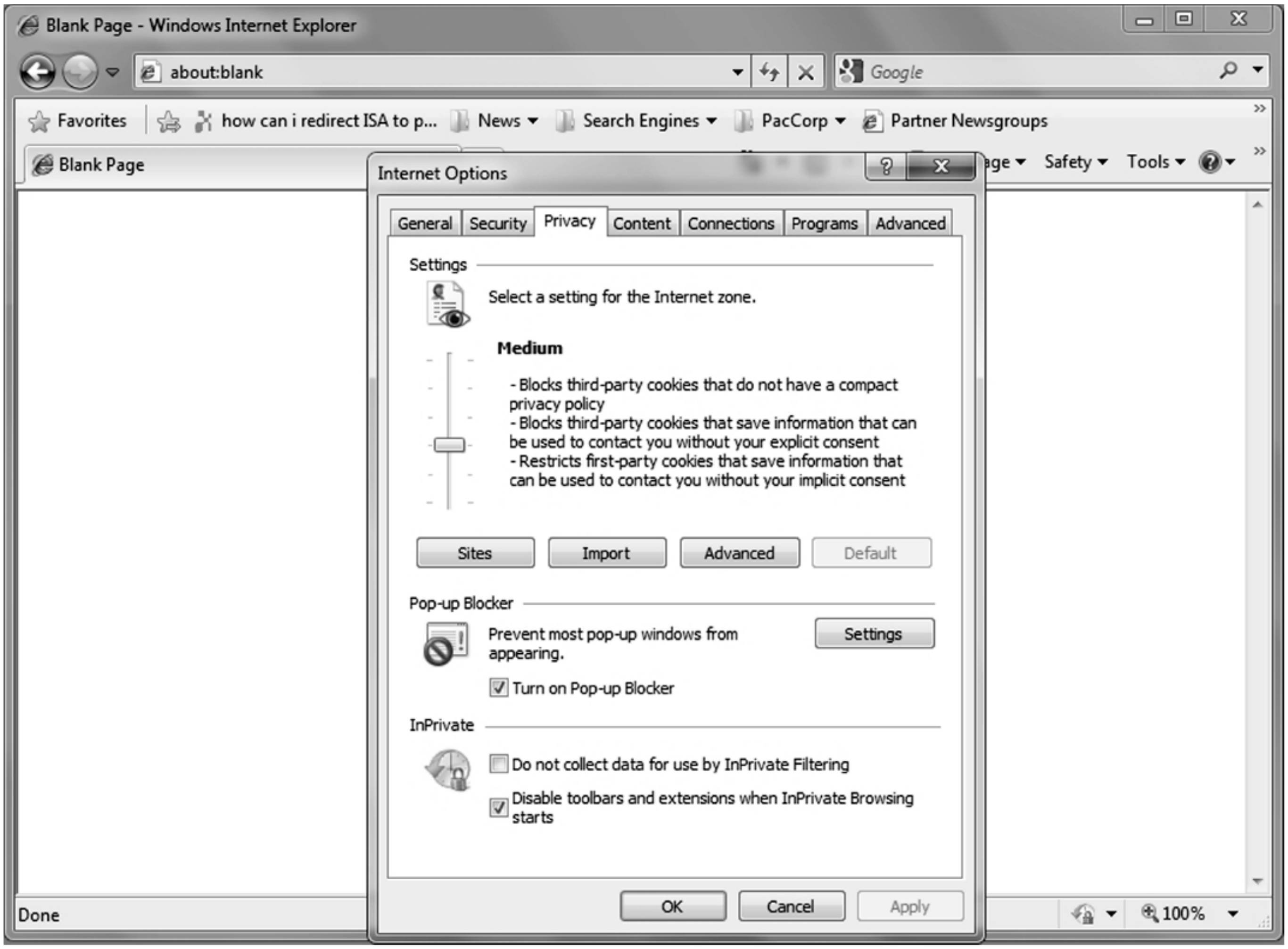
4. Select the **Cookies** check box, and then click **Delete** if it isn't already checked. Clear or select check boxes for any other information you also want to delete. If you want to keep cookies for your saved favorites, select the Preserve Favorites website data check box.

Being aware of how your private information is used when browsing the web is also important to help prevent targeted advertising, fraud, and identity theft. Here, it's important to use the appropriate privacy settings.

CHANGE PRIVACY SETTINGS

GET READY. To change Internet Explorer's privacy settings, perform these steps:

1. Open **Internet Explorer**.
2. Click the **Tools** button, and then click **Internet Options**.
3. Click the **Privacy tab**. See Figure 5-9.



Internet Options

General | Security | Privacy | Content | Connections | Programs | Advanced

Settings

Select a setting for the Internet zone.

Medium

- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that save information that can be used to contact you without your explicit consent
- Restricts first-party cookies that save information that can be used to contact you without your implicit consent

Sites | Import | Advanced | Default

Pop-up Blocker

Prevent most pop-up windows from appearing.

☑ Turn on Pop-up Blocker

InPrivate

□ Do not collect data for use by InPrivate Filtering

☑ Disable toolbars and extensions when InPrivate Browsing starts

Figure 5-9 Privacy tab

To adjust your privacy settings, adjust the slider to a new position on the privacy scale. The default level is Medium; it is recommended that you configure your settings for Medium or higher. If you click on the Advanced button, you can override certain settings, and if you click the Edit button, you can allow or block cookies from individual websites.

Pop-up windows are very common on the Internet. Although some pop-up windows are useful website controls, most are simply annoying advertisements, and a few may attempt to load spyware or other malicious programs. To protect your computer, Internet Explorer has the capability to suppress some or all pop-ups. To configure the pop-up blocker, use the following procedure:

This document belongs to VICTOR D AZULA (victorazula@hotmail.com) No unauthorized copies allowed!

CONFIGURE THE POP-UP BLOCKER

GET READY. Log on to Windows 7, then perform these steps:

1. Click **Start**, and click **Control Panel**. The **Control Panel** window appears.
2. Select **Network and Internet** > **Internet Options**. The Internet Properties sheet appears.
3. Click the **Privacy** tab. Make sure the **Turn on Pop-up Blocker** option is selected.
4. Click **Settings**. The Pop-Up Blocker Settings dialog box appears.

5. To allow pop-ups from a specific website, type the URL of the site in the **Address of website to allow text box**, and then click **Add**. Repeat the process to add additional sites to the Allowed sites list.

6. Adjust the Blocking level drop-down list to one of the following settings:

   - **High:** Block all pop-ups
   - **Medium:** Block most automatic pop-ups
   - **Low:** Allow pop-ups from secure sites

7. Click **Close** to close the Pop-Up Blocker Settings dialog box.

8. Click **OK** to close the **Internet Properties** sheet.

Examining Content Zones

To help manage security when visiting sites, Internet Explorer divides your network connection into four ***content zones*** or types. For each of these zones, a security level is assigned.

The security for each zone is assigned based on dangers associated with the zone. For example, it is assumed that when you connect to a server in your own corporation, you are safer than when connecting to a server on the Internet.

The four default content zones are as follows:

- **Internet zone:** This zone is used for anything that is not assigned to another zone and anything that is not on your computer or your organization’s network (intranet). The default security level of the Internet zone is Medium.
- **Local intranet zone:** This zone is used for sites that are part of an organization’s network (intranet) and do not require a proxy server, as defined by the system administrator. These include sites specified on the Connections tab, network, paths such as \\computername\foldername, and local intranet sites such as http://internal. You can add sites to this zone. The default security level for the Local intranet zone is Medium-Low, which means Internet Explorer will allow all cookies from websites in this zone to be saved on your computer and read by the website that created them. Finally, if the website requires NTLM or integrated authentication, it will automatically use your username and password.
- **Trusted sites zone:** This zone contains sites from which you believe you can download or run files without damaging your system. You can assign sites to this zone. The default security level for the Trusted sites zone is Low, which means Internet Explorer will allow all

cookies from websites in this zone to be saved on your computer and read by the website that created them.

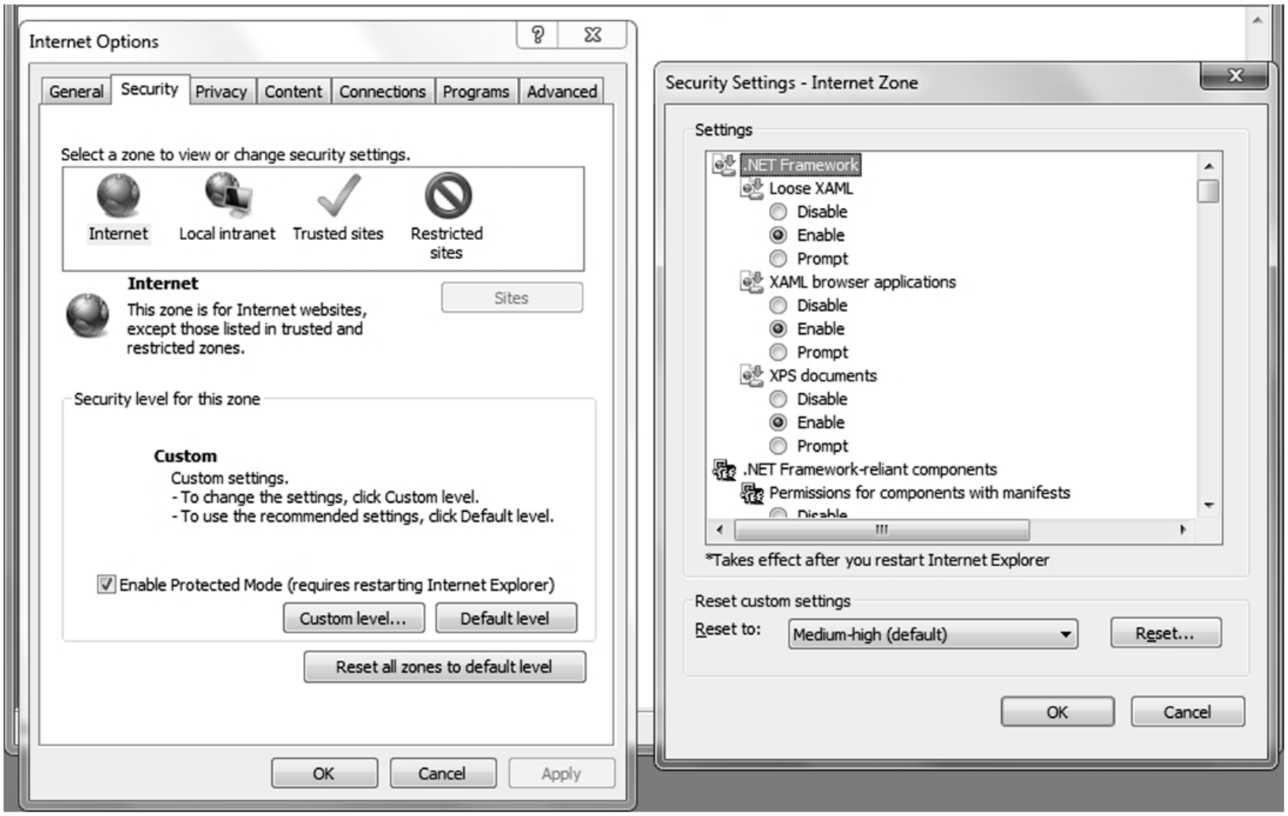
- **Restricted sites zone:** This zone contains sites that you do not trust and from which downloading or running files may damage your computer or data. These sites are considered a security risk. You can assign sites to this zone. The default security level for the Restricted sites zone is High, which means Internet Explorer will block all cookies from websites in this zone.

To tell which zone a web page falls into, look at the right side of the Internet Explorer status bar.

MODIFY SECURITY LEVEL FOR WEB CONTENT ZONE

GET READY. To modify the security level for a web content zone, perform these steps:

1. Click the **Tools** button, and then click **Internet Options**.
2. In the **Internet Options** dialog box, on the **Security** tab, click the zone on which you want to set the security level. See Figure 5-10.



Select a zone to view or change security settings.

Internet

This zone is for Internet websites, except those listed in trusted and restricted zones.

Security level for this zone

Custom

Custom settings.
- To change the settings, click Custom level.
- To use the recommended settings, click Default level.

☑ Enable Protected Mode (requires restarting Internet Explorer)

.NET Framework
- Loose XAML
  - ○ Disable
  - ● Enable
  - ○ Prompt
- XAML browser applications
  - ○ Disable
  - ● Enable
  - ○ Prompt
- XPS documents
  - ○ Disable
  - ● Enable
  - ○ Prompt

.NET Framework-reliant components
- Permissions for components with manifests
  - ○ Disable

*Takes effect after you restart Internet Explorer

Reset custom settings

Reset to: Medium-high (default)

Figure 5-10 Configuring security content zones

3. Drag the slider to set the security level to **High**, **Medium**, or **Low**. Internet Explorer describes each option to help you decide which level to choose. You will be prompted to

confirm any reduction in security level. You can also choose the **Custom Level** button for more detailed control.

4. Click **OK** to close the **Internet Options** dialog box.

For each of the web content zones, there is a default security level. The security levels available in Internet Explorer are as follows:

- **High:** Excludes any content that can damage your computer
- **Medium:** Warns you before running potentially damaging content
- **Low:** Does not warn you before running potentially damaging content
- **Custom:** A security setting of your own design

The easiest way to modify the security setting that Internet Explorer imposes on a specific website is to manually add the site to a security zone. The typical procedure is to add a site to the Trusted sites zone to increase its privileges, or to instead add it to the Restricted sites zone to reduce its privileges. To do this, use the following procedure:

ADD A SITE TO A SECURITY ZONE

GET READY. Log on to Windows 7, then perform these steps:

1. Click **Start**, and click **Control Panel**. The Control Panel window appears.
2. Select **Network and Internet** > **Internet Options**. The Internet Properties sheet appears.
3. Click the **Security** tab.
4. Select either the **Trusted sites** or **Restricted sites** zone to which you want to add a site.
5. Click **Sites**. The Trusted sites or Restricted sites dialog box appears.
6. Type the URL of the website you want to add to the zone into the **Add this website to the zone** text box, and then click **Add**. The URL appears in the Websites list.
7. Click **Close** to close the Trusted sites or Restricted sites dialog box.
8. Click **OK** to close the Internet Properties sheet.

To modify the security properties of a zone, use the following procedure:

MODIFY SECURITY ZONE SETTINGS

GET READY. Log on to Windows 7, then perform these steps:

1. Click **Start**, and click **Control Panel**. The Control Panel window appears.
2. Select **Network and Internet** > **Internet Options**. The Internet Properties sheet appears.
3. Click the **Security** tab.
4. Select the zone for which you want to modify the security settings.
5. In the **Security level for this zone** box, adjust the slider to increase or decrease the security level for the zone. Moving the slider up increases the protection for the zone, and moving the slider down decreases it.
6. Select or clear the **Enable protected mode** check box, if desired.
7. To exercise more precise control over the zone's security settings, click **Custom level**. The Security Settings dialog box for the zone appears.
8. Select radio buttons for the individual settings in each of the security categories. The radio buttons typically make it possible to enable a setting, disable it, or prompt the user before enabling it.
9. Click **OK** to close the Security Settings dialog box.
10. Click **OK** to close the Internet Properties sheet.

Phishing and Pharming

Phishing and pharming are two forms of attack used to lure individuals to bogus websites in an attempt to spread malware or collect personal information.

Phishing is a technique based on social engineering. With phishing, users are asked (usually through email or websites) to supply personal information in one of two ways:

- By replying to an email asking for their username, password, and other personal information, such as account numbers, PINs, and Social Security number
- By navigating to a convincing-looking website that urges them to supply their personal information, such as passwords and account numbers

For example, say you receive an email stating that your credit card account has just expired or that you need to validate your information. The email offers you a link to click on. When you click on the link, you go to the fake website. However, by “logging in” to the site with your real information, you are actually providing your username and password to the hacker, who can then use this information to access your account.

To help protect against phishing, Internet Explorer 8 includes SmartScreen Filter, which examines traffic for evidence of phishing activity and displays a warning to the user if it finds any. It also sends the address back to the Microsoft SmartScreen service for comparison against lists of known phishing and malware sites. If SmartScreen Filter discovers that a website you’re visiting is on the list of known malware or phishing sites, Internet Explorer will display a blocking webpage and the Address bar will appear in red. From the blocking page, you can choose to bypass the blocked website and go to your home page instead, or you can continue to the blocked website, although this is not recommended. If you decide to continue to the blocked website, the Address bar will continue to appear in red.

One of the best ways to avoid such ploys is to know that they exist. Accordingly, when you get an email requesting personal information, look for signs that the email is fake and that links within it go to bogus websites (e.g., instead of going to ebay.com, a link goes to ebay.com.com or ebay_ws-com). Don’t trust hyperlinks. Never supply a password or any other confidential information to a website unless you type the URL yourself and you are sure that it is correct.

Pharming is an attack aimed at redirecting a website’s traffic to a bogus website. This is usually accomplished by changing the hosts file (a text that provides name resolution for host or domain names to IP address) on a computer or by exploiting a vulnerability on a DNS server. To protect against pharming, you need to make sure your system has the newest security patches and that it is a up-to-date antivirus software package. In addition, UAC will help protect the hosts file since it is located in the System32 folder, which is one of the areas UAC helps protect.

Protecting Your Server

THE BOTTOM LINE

When considering security, remember that you need to secure your network, your clients, and your servers. By securing all three, you adopt a layered approach that makes it more difficult for hackers and malware to breach your organization. In previous lessons, we discussed how to keep your network secure. Earlier in this lesson, we discussed how to keep your clients secure. Now, in this portion of the lesson, we’ll focus on securing the server.

As you already know, servers are computers that are meant to provide network services and applications for your organization. Unlike a workstation, if a server fails, it will affect multiple users. Therefore, it is more important to keep a server more secure than a workstation.

Placing the Server

CERTIFICATION READY

Do you know how to protect your servers so that they are always up and running?

4.3

The first step in securing a server is determining where to place the server. Of course, the server should be kept in a secure location. In addition, servers should be on their own subnet and VLAN to reduce the traffic reaching them, including broadcasts.

In some instances, you may need to place servers at a branch office. In situations in which you need to install a domain controller in a low physical security environment, you should consider installing a Read-Only Domain Controller (RODC), which holds a nonwriteable copy of Active Directory and redirects all write attempts to a Full Domain Controller. This device replicates all accounts except sensitive ones. Therefore, if the domain controller is compromised, attackers are limited in what they can do when writing information to Active Directory.

Hardening the Server

The next step in securing a server is to harden the server to reduce the attack surface, thereby reducing the server's vulnerabilities. To harden a server, you should look for security guidelines and best practices for Windows servers and for the specific network services you are installing, such as Microsoft Exchange or Microsoft SQL Server.

One of the most important steps in securing a server is to make sure that Windows, Microsoft applications, and other network applications are kept current with the newest security patches. As with clients, you can do this using Windows updates, WSUS, and SCCM. Of course, before applying patches to a production system, make sure that you test the security updates.

To reduce a server's attack surface, you should disable any service that is not necessary so that this service cannot be exploited in the future. In addition, you should consider using host firewalls (such as Windows Firewall) that will block all ports that are not being used.

To reduce the effect of losing a server, you should separate the services. Never install all of your services on one server! You also need to plan for the rest and hope for the best. This means that you need to anticipate that a server will eventually fail. Therefore, you should consider using redundant power supplies, RAID disks, redundant network cards, and clusters.

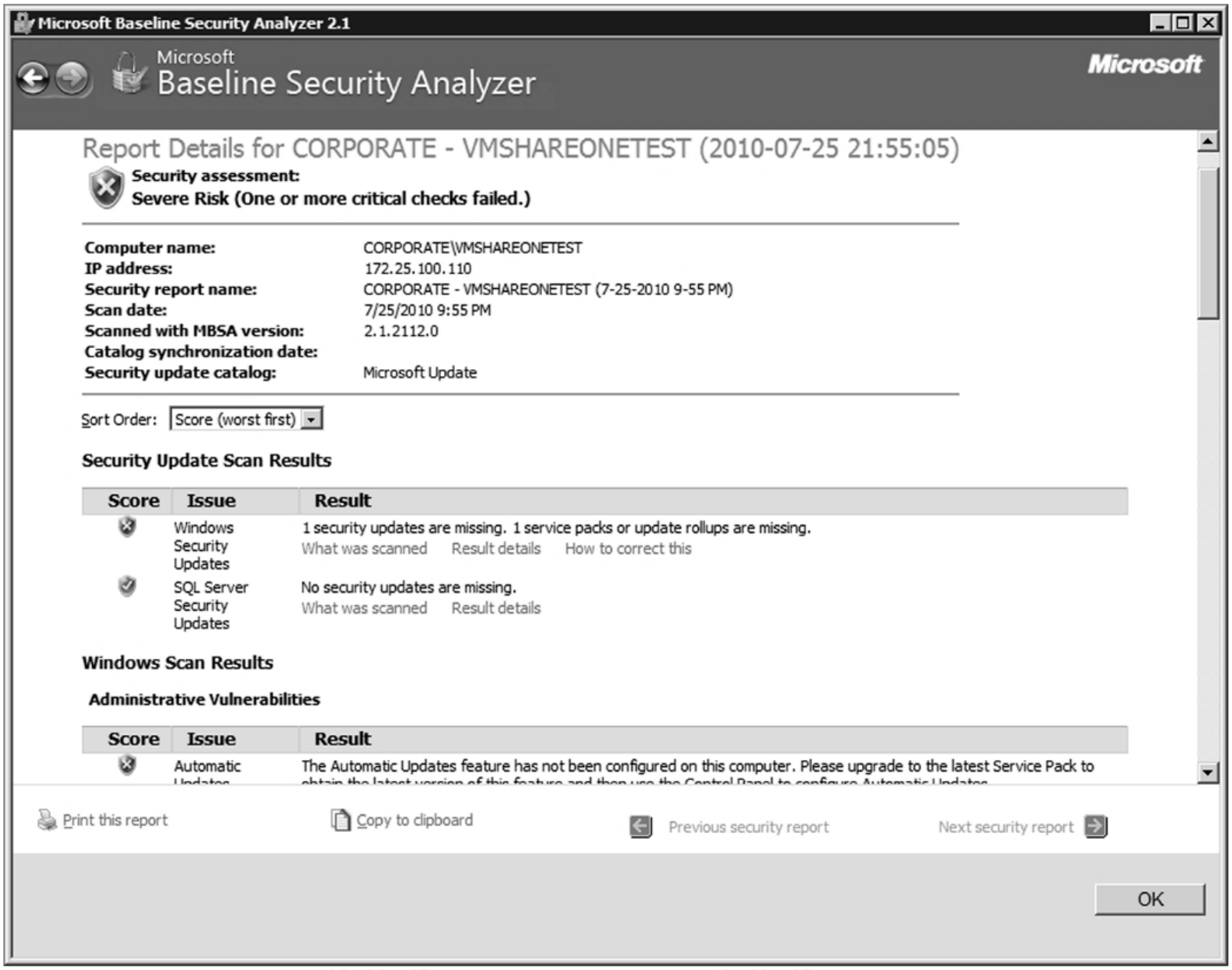
You should also disable or delete any unnecessary accounts. For example, although you cannot delete the administrator account, you can rename it to something else so that it will be more difficult for a hacker to guess what it is. In addition, you should not use the administrator account for everything. For example, if you have to run a specific service, create a service account for that service and give it the minimum rights and permissions that it needs to run. Of course, the guest account should be disabled.

Besides disabling or deleting any unnecessary accounts and only assigning the minimum rights and permissions necessary for users to do their jobs, you should also minimize who can log on locally to the server.

In addition, you should disable any unsecure authentication protocols. For example, you should not use Password Authentication Protocol (PAP) when using remote access protocols. You should not use FTP with passwords. Instead, use either anonymous that does not require passwords (assuming its content does not need to be secure) or use secure FTP, which will encrypt the password and content when being transmitted over the network. For similar reasons, you should not use telnet. Instead, use SSH.

Finally, you should enable a strong audit and logging policy and review these logs on a regular basis. If someone tries to hack a server or do something that he or she should not be doing, you will have a record of that person's activities. This should include both successful and failed account logins.

Microsoft Baseline Security Analyzer (MBSA) is a software tool released by Microsoft to determine the security state of a system by assessing missing security updates and less-secure security settings within Microsoft Windows components such as Internet Explorer, IIS web server, and products such as Microsoft SQL Server and Microsoft Office macro settings. See Figure 5-11.


Microsoft Baseline Security Analyzer 2.1
Microsoft
Baseline Security Analyzer
Microsoft

Report Details for CORPORATE - VMSHAREONETEST (2010-07-25 21:55:05)

Security assessment:
Severe Risk (One or more critical checks failed.)

Computer name:	CORPORATE\VMSHAREONETEST
IP address:	172.25.100.110
Security report name:	CORPORATE - VMSHAREONETEST (7-25-2010 9-55 PM)
Scan date:	7/25/2010 9:55 PM
Scanned with MBSA version:	2.1.2112.0
Catalog synchronization date:	
Security update catalog:	Microsoft Update

Sort Order: Score (worst first)

Security Update Scan Results

Score	Issue	Result
☒	Windows Security Updates	1 security updates are missing. 1 service packs or update rollups are missing. What was scanned Result details How to correct this
✓	SQL Server Security Updates	No security updates are missing. What was scanned Result details

Windows Scan Results

Administrative Vulnerabilities

Score	Issue	Result
☒	Automatic Updates	The Automatic Updates feature has not been configured on this computer. Please upgrade to the latest Service Pack to obtain the latest version of this feature and then use the Control Panel to configure Automatic Updates

Figure 5-11 Microsoft Baseline Security Analyzer

Microsoft often publishes security guides and best practices guides for various products. In addition, Microsoft has published the Threats and Countermeasures—Security Settings in Windows Server 2008 and Windows Vista, which can be found at **http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=037d908d-6a1c-4135-930c-e3a0d6a34239.**

Using Secure Dynamic DNS

> Since Windows Server 2003, Windows servers have provided support for the DNS dynamic update functionality. Dynamic DNS lets client computers dynamically update their resource records in DNS. When you use this functionality, you improve DNS administration by reducing the time that it takes to manually manage DNS zone records. You can use the DNS update functionality with DHCP to update resource records when a computer's IP address is changed.

With typical unsecured dynamic updates, any computer can create records on your DNS server, which leaves you open to malicious activity. To protect your DNS server, secure it so that only members of an Active Directory domain can create records on the server.

SKILL SUMMARY

IN THIS LESSON, YOU LEARNED:

- Because client computers are connected to an organization’s network and may have direct and indirect access to servers and network resources, it is important that these computers are protected.

- A virus is a program that can copy itself and infect a computer without the user’s consent or knowledge.

- A backdoor in a program gives remote, unauthorized control of a system or initiates an unauthorized task.

- Some viruses, worms, rootkits, spyware, and adware work by exploiting security holes in Windows, Internet Explorer, or Microsoft Office.

- The first step to protecting yourself against malware is keeping your Windows system (as well as other Microsoft products, such as Internet Explorer and Microsoft Office) up to date with the latest service packs, security patches, and other critical fixes.

- A virus hoax is a message warning the recipient of a nonexistent computer virus threat, usually sent as a chain email that tells the recipient to forward it to everyone he or she knows. This is a form of social engineering that plays on people’s ignorance and fear.

- User Account Control (UAC) is a feature that helps prevent malware. UAC was first introduced with Windows Vista and is included with Windows 7.

- Microsoft recommends that you always use Windows Firewall.

- Offline files are not encrypted unless you choose for them to be. You might opt to encrypt your offline files if they contain sensitive or confidential information and you want to make them more secure by restricting access to them.

- If you do not allow users to log on as administrators, you can limit what software these users install and you can better protect the system from malware.

- You can also use Group Policies to restrict what software can be executed on a client computer.

- Most email is unsolicited; such messages are called spam or junk email.

- The best place to establish a spam filtering system is on your email relay on a dedicated server or appliance, or as part of a firewall device or service.

- To make a spam message look like a legitimate message, sometimes spammers try to spoof an email address or IP address where a message comes from.

- Spammers look for unprotected SMTP servers to relay their emails through.

- Although some pop-up windows are useful web site controls, most are simply annoying advertisements, and a few attempt to load spyware or other malicious programs.

- To help manage security when visiting websites, Internet Explorer divides your network connection into four content zones or types. Each of these zones is assigned a security level.

- Phishing and pharming are two forms of attack used to lure individuals to bogus websites in an attempt to spread malware or collect personal information.

- All servers should be kept in a secure location. In addition, servers should be on their own subnet and VLAN to reduce the traffic reaching them, including broadcasts.

- You should also secure a server by hardening it to reduce the attack surface. When hardening a server, look for security guides and best practices for Windows servers, as well as for the specific network services you are installing.

- To secure your DNS server, make it so that only members of an Active Directory domain can create records on the DNS server.

Knowledge Assessment

Multiple Choice

Circle the letter that corresponds to the best answer.

1. Which type of malware copies itself onto other computers without the owner's consent and will often delete or corrupt files?

a. Virus

b. Worm

c. Trojan horse

d. Spyware

2. Which type of malware collects personal information or browsing history, often without the user's knowledge?

a. Virus

b. Worm

c. Trojan horse

d. Spyware

3. Your computer seems to be slow, and you notice that you have a different default web page than usual. What is most likely the cause of problems?

a. Your ISP has slowed your network connection.

b. Your computer has been infected with malware.

c. You did not update your computer.

d. You accidentally clicked the turbo button.

4. Besides installing an antivirus software package, you should always ___________ to protect your computer against malware.

a. keep your machine up to date with the latest security patches

b. reboot your computer on a regular basis

c. change your password on a regular basis

d. spoof your IP address

5. A thoroughly tested, cumulative set of hotfixes and other patches is known as a ___________.

a. Recommended update

b. Hotfix pack

c. Service pack

d. Critical update

6. What technology is used by Windows to prevent unauthorized changes to your system?

a. UAC

b. Protected mode

c. Windows Defender

d. ProtectGuard

7. When using UAC, which of the following requires administrative permissions or rights?

a. Installing updates from Windows update

b. Changing the date and time

c. Resetting the network adapter

d. Installing drivers from Windows update or attached with the operating system

8. What mechanism is working when you try to change a computer's display settings and you get a pop-up asking whether you wish to continue?

a. Windows Firewall

b. Protected Mode

c. Windows Update

d. UAC

9. What host-based firewall software comes with current versions of Windows?

a. Windows Firewall

b. Windows Protected Mode

c. UAC

d. Windows GuardIt

10. What program would you use to configure IPsec on a computer running Windows Server 2008?

a. Windows Firewall with IPsec Plugin

b. IPsec Monitor

c. Windows with Advanced Security

d. IPsec Configuration console

11. If you have sensitive or confidential information stored in your offline files, it is recommended that you

a. Clear your cache

b. Encrypt the offline files

c. Clear your cookies

d. Execute ipconfig /renewip

12. You determine that legitimate emails are being blocked by your spam-blocking device. What should you do?

a. Flush out the quarantined items

b. Reboot the spam-blocking device

c. Add the address or domain for these emails to the white list

d. Add the address or domain for these emails to the black list

13. SMTP uses TCP port ___________.

a. 43

b. 25

c. 80

d. 443

14. How many content zones are there in Internet Explorer?

a. 1

b. 2

c. 4

d. 8

15. Say that you receive an email stating that your account has just expired and asking you to log in to a legitimate-looking website to fix the problem. This is most likely an instance of ___________.

a. Phishing

b. Pharming

c. Phaking

d. IP address spoofing

Fill in the Blank

Complete the following sentences by writing the correct word or words in the blanks provided.

1. _________ is software that is designed to infiltrate or infect a computer, usually with ill intent.

2. A(n) _________ is a self-replicating program that copies itself to other computers while consuming network resources.

3. Microsoft's antispyware program is called _________.

4. For antivirus software to be effective, it must be kept _________.

5. An example of a(n) _________ is a message saying to delete the win.com file because it is a virus.

6. If you want to control what updates get pushed to clients within your organization, you would use _________ or _________.

7. _________ is when you are asked if you want to continue with an action and your desktop is dimmed and other programs are temporary halted until you approve the change.

8. _________ are copies of network files that are stored on your computer so that you can access them when you are not connected to the network.

9. _________ is another name for junk email.

10. _________ is an email validation system that is designed to verify that an email is coming from the proper email server.

Competency Assessment

Scenario 5-1: Checking Physical Security

You were just hired as an IT administrator for the ABC Company. Across from your desk, there is a table with seven physical servers. You go to your boss and ask why the servers are out in the open and not locked up. He says there are located on the table so that they can be easily monitored and watched. How should you respond to your boss?

Scenario 5-2: Programming Backdoors

You have been hired as a security consultant for the Contoso Corporation. One day, you are working with the CIO on a new comprehensive security policy for the company. Although the CIO is not a programmer herself, she wants to understand how she can keep programmers from creating a backdoor on the programs they create for the company. What do you tell her?

Proficiency Assessment

Scenario 5-3: Scanning with Microsoft Baseline Security Analyzer

Download and install the newest Microsoft Baseline Security Analyzer on a Windows server, then scan the computer for missing security updates and less-optimal security settings.

Scenario 5-4: Looking at Windows Updates

Go to **http://www.microsoft.com/technet/security/bulletin/advance.mspx.** Read the most recent advance notification or most recent security bulletin summary and review the executive summary. Determine how many security bulletins there are for the most recent month. Then run Windows Update to bring your system up to date with the newest patches.

Workplace Ready

Keeping Up with Security

Maintaining security for an organization is often a full-time job that usually requires multiple people with various skill sets. For example, you may have a person who is responsible for routers and firewalls, another person who is responsible for servers, and another person who is responsible for client computers. You may also have a security manager who oversees all items related to security, including physical security. Of course, a company's CEO, CIO, and other executives are the ones who are ultimately responsible for security.

However, for security to be effective, you need to remember that everyone needs to participate. This includes the executives who support the IT department and help enforce and support security-related decisions, as well as the IT staff members who establish the security measures and monitor them. But don't forget that the weakest link could be the end user. Best practices, awareness training, and constant reminders are key to communicating to all employees why security is so important.