Global Information Assurance Certification Paper

A Novice's Guide to Securing Windows XP Home Edition

GSEC Version 1.4b Option 1

Jessica Deline

Contents

Abstract
It can be frustrating for a novice interested in securing their computer running Windows XP Home Edition (HE) to find a concise guide. This one is intended for a typical home user that is connected to the Internet via a broadband connection such as a cable modem or DSL. While it is easy to find tips on securing your computer; a search on Google using the key words “guide securing Windows XP Home Edition” does produce a wealth of material. The problem is that many of the guides that purport to be applicable to the Home Edition of Windows XP describe many procedures that can only be carried out on Windows XP Professional. In addition, Windows XP HE exposes features of the Professional version interface that are broken and will not function properly. The purpose of this step-by-step guide is to outline the basic procedures required to secure Windows XP Home Edition. When expedient, variations from well-known best practices will be highlighted and differences between Home Edition and Professional will be explained. Topics that are covered include: security update management, user management, file and folder management, personal firewall implementation, establishing a TCP/IP port activity baseline, virus protection, configuring a secure OS, configuring networking security, auditing security events, and backups.

Security Update Management

The first step to securing Windows XP Home Edition is to make sure that your operating system is not vulnerable to widely publicized exploits. Microsoft provides three means of achieving this goal. The most basic procedure is to point your web browser to http://windowsupdate.microsoft.com. [1] Windows Update will scan your computer and provide you with a list of critical updates and service packs, recommended downloads, and driver updates. Click the Scan for updates link to begin the process. In order to secure your system, you must be sure to install all of the critical updates and service packs. The recommended downloads and driver updates are strictly optional.

The second step to take for a home user with a cable modem or DSL connection to the Internet is to take advantage of the Automatic Updates component of Windows XP Home Edition to insure that critical updates and service packs are applied in a timely fashion. To turn on Automatic Updates, click Start | Control Panel and then click the Performance and Maintenance link. Click the System icon and then select the Automatic Updates tab. Be sure that the Keep my computer up to date check box is selected. That way whenever you connect to the Internet, your computer will check the Windows Update site for the latest Windows, Microsoft Internet Explorer, Microsoft Media Player, and selected updates and download them automatically for you. There are three possible Automatic Updates settings to choose from: Download the updates automatically and notify me when they are ready to be installed (default); notify me before downloading any updates and notify me again before installing them on my computer; and turn off automatic updating. I recommend choosing the default setting of Downloading the updates automatically. However, since some updates have flaws that can interfere with the functioning of installed applications; you should manually set a restore point before proceeding with the installation.

The third means of securing your system against known exploits involves installing the Microsoft Baseline Security Analyzer (MBSA), available for download at http://download.microsoft.com/download/e/5/7/e57f498f-2468-4905-aa5f-369252f8b15c/mbsasetup.msi. [2] The MBSA is a graphic program that runs hfnetchk (a command-line tool that assesses your computer for the absence of security patches) and scans for additional vulnerabilities. Besides checking for missing service packs and hotfixes, the MBSA scans for security misconfigurations in Windows NT 4.0, Windows 2000, Windows XP, Microsoft Internet Information Services (IIS) 4.0 and 5.0, Microsoft Internet Explorer (IE) 5.01+, Microsoft SQL Server 7.0 and 2000, Exchange 5.5 and 2000, and Windows Media Player 6.4+.

It is important to point out that many security guides that I have reviewed stress the importance of downloading and running hfnetchk. However, the program that is available for download is not the latest version. Microsoft is in the process of removing hfnetchk as a stand-alone offering since the MBSA can perform security scans, and the latest version of hfnetchk is only available by installing the MBSA program. [3] To run the version of hfnetchk that is bundled with the MBSA you open a command prompt and navigate to the MBSA installation folder. Then type the following command "mbsacli.exe /hf –v –z –s 1" without the quotes and press ENTER. Here is an example of the results:

```
Done scanning MYCOMPUTER
---------------------------
MYCOMPUTER (127.0.0.1)
---------------------------

  * WINDOWS XP SP1

  Warning         MS02-055        323255
  File C:\WINDOWS\system32\hhctrl.ocx has a file version [5.2.3735.0]
  greater than what is expected [5.2.3669.0].


  * INTERNET EXPLORER 6 SP1

  Information
  All necessary hotfixes have been applied.

  * WINDOWS MEDIA PLAYER 9.0

  Information
  There are no entries for this product in the XML file.
```

Hfnetchk examines several values before it reports on the status of a patch. The registry key that is associated with the patch is checked first. If the registry key does not exist on your computer, the patch is considered not to be installed. If the key does not exist, Hfnetchk examines the file version and file checksum for each file in the hotfix. If all of these values match, the patch is considered to be installed. If any one of these tests does not work, the patch is either considered to be not installed, or it is flagged as a warning. [4] The warning in the Windows XP SP1 section above refers to Security Bulletin MS02-055. All referenced bulletins can be found at

http://www.microsoft.com/technet/security/current.asp. [5] The Windows Media Player 9.0 section indicates that no entries for this product exist in the XML file. That means that since I'm running beta software, hfnetchk is not able to scan for vulnerabilities.

The Microsoft Baseline Security Analyzer adds additional capabilities to hfnetchk. It examines Windows desktops and servers for common security best practices such as strong passwords, scanning IIS and SQL Server for security misconfigurations, and checking for misconfigured security zone settings in Microsoft Office, Outlook, and Internet Explorer. When a vulnerability is found, the MBSA reports what was scanned, results details, and how to correct the issue.

User Management

According to the principle of least privilege, the users of a computer system should have only the minimal access rights needed to perform their duties. In order to secure our installation of Windows XP Home Edition, we are going to apply this principle. It is important that only two user accounts (the built-in Administrator [Owner] account and one user account such as USERNAME) have unlimited power to manipulate the computer. This will help prevent inexperienced users from installing poorly written and/or malicious programs and device drivers that cause the system to crash.

There are only two kinds of accounts in Windows XP Home Edition. First, there is a computer administrator account. This type of account has unlimited power to modify the computer in any way and to view and alter the contents of all other accounts. The built-in administrator account (Owner) is this type of account. All subsequently created accounts are initially computer administrator accounts also. But, you can change their account type after creation. Specific rights for the administrator include the ability to: create and delete other computer accounts on the computer; change any user's account name, picture, password, and account type; install and uninstall software and hardware, and change all system-wide settings. Note: the built-in administrator account (Owner) cannot be changed to any other type. This is to ensure that there is always someone able to fully operate the computer.

This second type of account in Windows XP Home Edition is a limited account placed in the Restricted Users local group. Assigning limited user accounts is recommended as an effective way to prevent inexperienced or unauthorized users from changing computer settings or deleting important files. Holders of limited accounts have the following abilities: create, change, or delete their account password; and change their account picture.

As I mentioned previously, each newly-created interactive user in XP Home Edition has an account type of computer administrator and is a member of the Owners local group, (which is the Windows XP HE equivalent of the Windows 2000 local Administrators group). The Backup Operators, Power Users, and Replicator groups from Windows 2000/XP Pro are missing from Home Edition, and the new group, Restricted Users, is added. [6] Restricted Users is the group that contains all limited accounts.

The next recommendation for securing Windows XP Home Edition is to immediately change all accounts but the one belonging to the user who is responsible for securing the computer (e.g., USERNAME) to a limited type account. Remember, you will also have the built-in Administrator (Owner) account as a member of the local Administrators group. To change another user's account type from administrator to limited, you click Start | Control Panel | User Accounts. Click the account you'd like to change under the pick an account to change section of the window. Next click the Change the account type link. Select the Limited radio button and then click the Change Account Type button.

By default, Windows XP Home Edition boots to a Welcome screen with a list of user accounts (except the built-in Administrator) and you just click on the account you want to access. But, you can configure Windows XP HE to use the classic logon and shutdown screens for every login session. Just click Start | Control Panel and then click User Accounts. Click Change the way users log on or off. Clear the Use the Welcome screen check box. However, if you disable the Welcome screen, you also disable Fast User Switching.

If you are concerned about your users introducing Trojan horse programs, you can even require users to press CTRL+ALT+DEL before the classic logon screen is displayed. Just click Start | Run and type regedit. Select the Winlogon subkey at HKLM\Software\Microsoft\WindowsNT\CurrentVersion\WinLogon. Click Edit | New and choose a DWORD value. Change the name to DisableCAD and press ENTER. Keep the data value set to 0 [0x0000000(0)].

File and Folder Management

The first step in protecting files and folders in Windows XP Home Edition requires that you check the file system of your computer's partitions. Although you can choose to format the disk partitions on a Windows XP HE computer as FAT (file allocation table), FAT32, or NTFS, the latter is the recommended file system. Only NTFS allows for both file and folder access control and supports limited accounts. Therefore it is imperative that all disk partitions on a Windows XP HE machine be formatted NTFS.

To check the format of a partition, click Start | Control Panel and then click the Performance and Maintenance link. Click the Administrative Tools link and then the Computer Management shortcut. Click the Disk Management object in the left pane to check the file system.

If you find that your partitions are FAT32 instead of NTFS, you can convert the partitions to NTFS using a command line utility, convert. Convert.exe converts volumes leaving existing files and folders intact. Convert will need exclusive access to the partition, so if you are converting the C: drive, a reboot will be required to complete the conversion.

Then next step in file and folder management is to set a password on all accounts. This is due to the file sharing mechanism that is implemented in Home Edition. Once a

password is assigned to an account, you gain the ability to designate any folder in your user profile as a private folder.

To add a password to an account, click Start | Control Panel | User Accounts. Click the account you'd like to change under the pick an account to change section of the window. Click the Create a password link. Type the new password and then confirm it. Leave the password hint text box blank on administrator type accounts (unless you want to make it easier for intruders to guess your password). You might consider filling in the text box for limited account types, especially if you have users who are not used to using passwords to access computing resources. If you do allow hints, be sure to construct extremely vague ones.

Under the default configuration, the built-in Administrator account (Owner) is not exposed when you access the User Accounts feature in Control Panel, you will only see the subsequently created accounts and the Guest account listed. To set a password on the built-in Administrator account, Click Start | Run and then type "control userpasswords2" without the quotes and click enter. In the User Accounts dialog box, click the Reset Password button to change the password for Administrator.

Unfortunately, you cannot administratively enforce strong passwords on Windows XP Home Edition. Instead, you will need to educate the users in your home about how to create a complex password. Some very interesting suggestions for creating good passwords can be found at http://online.securityfocus.com/infocus/1554/. [7]

Once passwords are setup on accounts, any user can make any folder in their user profile private. The user profile includes My Documents and its subfolders, Desktop, Start Menu, and Favorites. When anyone makes a folder private, all the files and folders it contains are private as well. To make a folder private, right-click a folder in your user profile and select Sharing and Security from the popup menu. Check the Make this folder private checkbox and click OK. When you complete this procedure, the security settings will be changed to SYSTEM Full Control and User (e.g., USERNAME) Full Control. Thus, even other administrative accounts will not have access to your private folder.

If you want to view the folder settings on a folder that you have made private, you cannot do so while logged in normally. To set, view, change, or remove file and folder permissions in Windows XP Home Edition, you must first boot into safe mode. Be sure to login as the built-in Administrator account (Owner). Now the security tab will be visible when viewing the properties of a file or folder. [8]

It is well known that deleting files on Windows operating systems does not erase the data. Rather, the area of the disk is marked as being ready for use. The possibility exists for the data to not be overwritten or to be partially overwritten by other data added later. This means that an intruder can potentially gain access to sensitive data left on the drive even after deletion.

In order to protect your "deleted" data from prying eyes, you might want to consider purchasing a program that can overwrite unused areas of the disk with 1's, and 0's. For example, BCWipe, 1 license (on a per-computer basis), costs $39.95. The BCWipe software is intended to give you confidence that erased files cannot be recovered by an intruder. The program can be run from My Computer as well as from a command prompt. BCWipe complies with US DoD 5200.28-STD and the Peter Gutmann wiping scheme. Information is available at http://www.jetico.com/index.htm#/bcwipe.htm [9]
In order to facilitate the management of files and folders, you should configure Windows Explorer to show additional information that is hidden by default. In Windows Explorer, click Tools | Folder Options and select the View tab. Make sure that Display the full path in the address bar and Display the full path in the title bar are checked. Make sure that the Show hidden files and folders radio button is selected. Make sure that the Hide extensions for known file types and the Hide protected operating system files (Recommended) check boxes are cleared. Also, make sure that Show file attributes in Detail View is checked. These settings will allow view all attributes, extensions, and properties of files and will aid in file and folder management, as well as in the investigation of a security incident.

Personal Firewall Implementation
Windows XP Home Edition includes Internet Connection Firewall (ICF) software that can be used as a personal firewall. ICF can be used to protect what information is being communicated between your home network, or single computer with cable modem, and the Internet. ICF should not be enabled on any connection that is not directly connected to the Internet. In other words, if the computer is on a home network where there is already a firewall present, or is using a modem to connect to an ISP, you should not enable ICF.

To enable ICF, click Start | Control Panel | Network Connections and then select the connection you want to protect. Then under Network Tasks click Change settings of this connection. On the Advanced tab, under Internet Connection Firewall, select the Protect my computer and network by limiting or preventing access to this computer from the Internet check box.

ICF is a "stateful" firewall. A stateful firewall is one that monitors all aspects of the communication that crosses its path and inspects the source and destination address of each message that the firewall handles. To prevent unsolicited traffic from the public side of the connection from entering the private side, ICF keeps a table of all communications that have originated from the computer that is running ICF. The ICF compares all inbound traffic from the Internet to the entries in the table. Inbound Internet traffic is permitted to pass the firewall only if there is a matching entry in the table that shows that the communication exchange *began* in your computer of private network. [10]

Communications that originate from a source outside the computer that is running ICF are dropped by the firewall unless you create an entry on the Services tab to allow passage. ICF does not send notifications about activity to the user, unsolicited

communications are silently discarded. This behavior of ICF would stop common hacking attempts such as port scanning. However, ICF can create a security log so that you can view the activity that is tracked by the firewall.

You can configure services so that unsolicited traffic from the Internet is forwarded by the computer that is running ICF to either itself or a home network. The ICF needs operational information (a service definition) to permit the unsolicited traffic to be forwarded into your network.

Protocols that are preconfigured on the Services tab of the ICF Advanced settings include: FTP, IMAP (3 & 4), SMTP, POP3, HTTPS, Telnet server, HTTP, and remote desktop. Installing Windows Messenger will add four additional services. Also, you can create service definitions by clicking the Add button. Then you give a description of the service, the name or IP address of the computer hosting the service on the network, the external port number for the service or the internal port number, and whether it is TCP or UDP. You have the option of editing an existing service in case the machine that is hosting the service is not the one that has ICF running.

You can use the Internet Connection Firewall settings security logging feature to create a security log of firewall activity. ICF can log both traffic that is permitted and traffic that is rejected. For example, by default, ICMP echo requests are not permitted and a log entry will appear for every unsuccessful inbound attempt. Also, you can set the size of the security log to prevent an overflow that might be caused by DoS attacks. In addition, it is possible to locate the log file (pfirewall.log) in any folder you desire.

Even though the built-in Internet Connection Firewall is regarded as an excellent personal firewall, the lack of granular control makes ICF too restrictive for some power users. To review, ICF is a stateful packet filter. By default ICF denies all traffic from the Internet. In addition, you can modify the ruleset to allow your computer to host services such as http or ftp. However, you cannot create a rule which opens up port 80 (Web services) to a particular IP address. If you punch a hole in ICF to port 80, then you are opening it up to the world. ICF does enforce a three-way handshake, it blocks packets that have impossible flag options set (e.g., a packet with both SYN and FYN bits), and it prevents IP spoofing using Raw Sockets and the IP_HDRINCL option. [11]

But, ICF does have its shortcomings. For example, there is no egress filtering available with ICF. So, an e-mail based Trojan attack, if successful, would have no problem opening up a connection with a computer on the Internet. The connection would originate within the PC, so ICF would let it pass. Another shortcoming is the fact that ICF lacks any real-time notification. Finally, ICF can only be installed on your home network on the machine directly connected to the Internet because it breaks file sharing and message notification. [12]

Therefore, a power user will want to install a more robust personal firewall such as the free-for-personal use ZoneAlarm. I downloaded ZoneAlarm 3.1.395 from

http://download.com.com/3000-2092-10039884.html?part=zonealarm&subj=dlpage&tag=button. [13]

After you install ZoneAlarm, from time to time you will see a Program Alert pop up on the screen. These program alerts will occur whenever one of your programs tries to access the Internet. The alert will include the destination IP address and the filename of the program that is attempting to make contact. So, the first time that iexplore.exe attempts to connect to the Internet, you can check the box "Remember the answer each time I use this program" and you will not be prompted with another alert. Before checking this box, you must be absolutely sure that you do want to allow the program to initiate outbound communications.

In the Programs panel of Zone Alarm, the list of program alerts can be reviewed. A green check mark indicates that the program is always allowed to connect, a question mark means that the program will ask every time it is started, and a red X means that the program will never be allowed to connect to the Internet. You can set different settings for the Internet and the Local zone (home network).

By default, ZoneAlarm blocks all incoming and outgoing traffic unless you explicitly allow a connection (by designating trusted programs as described above). The Firewall alert feature can be configured to tell you whenever unauthorized communication tries to get into your computer. ZoneAlarm automatically blocks unauthorized incoming traffic, but you can use the Firewall alert feature as a real-time monitoring program to aggressively respond to threats. All incoming traffic is identified by IP address so that you can use a program like Sam Spade (http://samspade.org [14]) to track down the source of suspicious activity.

Establishing a TCP/IP Port Activity Baseline

One of the difficulties associated with the application of egress filtering using ZoneAlarm is that the typical user will be confronted with a Program Alert indicating that svchost.exe, or some other program unfamiliar to them, wants to establish an outbound connection. In order to make intelligent decisions about whether to allow the connection this one time or each time you use the program, you must establish a baseline of legitimate TCP/IP activity.

The version of NETSTAT that comes with Windows XP has a switch that is extremely useful for establishing the baseline that will be used to help implement egress filtering. Security professionals are quite familiar with the –a switch for NETSTAT that displays all connections and listening ports and the –n switch that displays the addresses and port numbers in numerical form. But, there is a new switch in the Windows XP version, -o, that displays the owning process ID associated with each connection. Here's an example of output from NETSTAT –ano:

```
Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       700
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
```

```
TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING       752
TCP    0.0.0.0:1026           0.0.0.0:0              LISTENING       4
TCP    0.0.0.0:3024           0.0.0.0:0              LISTENING       1308
TCP    0.0.0.0:5000           0.0.0.0:0              LISTENING       960
TCP    192.168.1.2:139        0.0.0.0:0              LISTENING       4
TCP    192.168.1.2:3024       192.168.20.2:1863      ESTABLISHED     1308
TCP    192.168.1.2:3025       192.168.10.1:53        TIME_WAIT       0
TCP    192.168.1.2:3032       192.168.10.1:53        TIME_WAIT       0
TCP    192.168.1.2:3034       192.168.20.2:80        TIME_WAIT       0
TCP    192.168.1.2:15678      0.0.0.0:0              LISTENING       1308
TCP    127.0.0.1:3001         0.0.0.0:0              LISTENING       1284
TCP    127.0.0.1:3002         0.0.0.0:0              LISTENING       752
TCP    127.0.0.1:3003         0.0.0.0:0              LISTENING       752
TCP    127.0.0.1:3008         0.0.0.0:0              LISTENING       1200
UDP    0.0.0.0:135            *:*                                    700
UDP    0.0.0.0:445            *:*                                    4
UDP    0.0.0.0:500            *:*                                    540
UDP    0.0.0.0:3004           *:*                                    752
UDP    0.0.0.0:3009           *:*                                    1308
UDP    0.0.0.0:3010           *:*                                    932
UDP    0.0.0.0:3011           *:*                                    932
UDP    192.168.1.2:123        *:*                                    752
UDP    192.168.1.2:137        *:*                                    4
UDP    192.168.1.2:138        *:*                                    4
UDP    192.168.1.2:1900       *:*                                    960
UDP    192.168.1.2:6976       *:*                                    1308
UDP    192.168.1.2:7122       *:*                                    1308
UDP    127.0.0.1:123          *:*                                    752
UDP    127.0.0.1:1900         *:*                                    960
```

Now that you have a list of active TCP/IP ports and process IDs, we just need to correlate the PIDs with the handles and dll processes that have opened them. That way we can determine if the process is legitimate and should be allowed to initiate any connections with other devices on the Internet. I use a freeware utility from Sysinternals called Process Explorer to quickly determine the processes running on the computer. You can download Process Explorer from http://www.sysinternals.com/ntw2k/freeware/procexp.shtml. [15]

So, in the above example, process 700 is listening on port 135 TCP. By consulting a list of well-known ports, I determine that 135 TCP is typically used for DCE endpoint resolution. [16] Next I view a list of ports used by Microsoft products and discover that Windows XP Home Edition probably uses this port for client/server communication. [17] Next I run Process explorer and determine that process 700 is being used by svchost.exe, the Generic Host Process for Win32 Services. My research shows that svchost.exe checks the services portion of the registry at startup to construct a list of services that it needs to load and that there can be multiple instances of svchost running concurrently. [18]

Therefore, after completing my investigation, I conclude that svchost.exe is supposed to be running on my Windows XP Home Edition PC. Therefore, if svchost.exe attempts to connect to the Internet and a ZoneAlarm Program Alert asks me if I want to allow it to do so, I can answer in the affirmative. Of course, I will need to repeat the above steps for each line in the NETSTAT –ano printout in order to generate my list of privileged

programs. But, if a program not on the list ever appears on a Program Alert, I can immediately suspect a possible system compromise.

Virus Protection

One of the items on Microsoft's Windows XP Home Edition Baseline Security Checklist is installing antivirus software and keeping it updated. [19] All systems connected to the Internet should have antivirus software installed, so that is the next step to take to secure your Windows XP HE computer. My PC is running Norton AntiVirus 2003 and the virus definitions are updated on a weekly basis. In addition, the LiveUpdate feature of NAV 2003 allows you to configure it to check the Internet every four hours and automatically update when new antivirus definitions are found. So, I have that configured as a backup in case I forget to update them manually.

Configuring a Secure OS

There is a principle called security through obscurity. The idea is to make a hacker work hard to compromise your computer in the hopes that they will give up and look for easier boxes to hack. One technique that follows this example is to rename the local Administrator (Owner) account to something not easily guessed. Click Start | Run and then type control userpasswords2 and click ENTER. Select the Administrator account and click Properties. In the User name text box, change Administrator to whatever you want (e.g., Ratdog). It is important to complete this step since this account cannot be disabled or locked out. Likewise you can rename the built-in Guest account using the same process.

Some security guides mention the technique of creating a bogus Administrator account and disabling it. That way the security logs will show when someone's been attempting to hack into the computer. Unfortunately, you cannot duplicate this procedure in Windows XP Home Edition. That is because the only user account that can be disabled is the built-in Guest account. If you do create a bogus Administrator account, you will be forced to make it a limited type account and give it an extremely complex password. Therefore, I cannot recommend this technique.

Oftentimes, steps are taken to prevent the installation of a rogue operating system, or to prevent the introduction of a virus, by making sure that the system boots from the hard drive first, and then the floppy drive and CD-ROM. The instructions for changing the boot order differ between computers. For many computers, after powering on the system, you press the DEL or the F2 key to enter the System Setup. Locate the Boot Sequence value and make sure that the Internal HDD is selected as the first (or only) boot device.

The Active Desktop feature of Windows XP Home Edition allows for web content to be integrated into the user interface. You might want to limit the ability of the users of your system to experiment with this feature. I recommend using Tweak UI to accomplish this. Tweak UI is one of the programs in the Power Toys for Windows XP suite available for download at http://www.microsoft.com/windowsxp/pro/downloads/powertoys.asp. [20] This program gives you access to system settings that are not available in the default

Windows XP user interface, including mouse settings, Explorer settings, taskbar settings, and more. To disallow Web content from being added to the desktop, click Start | Programs | Powertoys for Windows XP | Tweak UI for Windows XP. Click on the Explorer object in the left pane. Clear the Allow Web content to be added to the desktop. This is a per-user setting and will need to be configured for each user. If you want to place Web content on the desktop, but want to prevent other users from adding content, you can enable the Lock Web content option.

Autoplay is the feature that allows for automatic activation of a program when a CD-ROM compact disc is inserted into the CD-ROM drive. Note: many people refer to this feature as AutoRun. The danger in allowing Autoplay is that you run the risk of inserting a CD with an autorun.inf file designed to automatically deliver a virus or malware like a Trojan horse to your computer. Therefore, it is a recommended practice to disable Autoplay. In order to complete this objective in Windows XP Home Edition, you must edit the registry. Therefore, I will highlight a method to complete this task that does not require manually editing the registry. Again, you use the Tweak UI utility. Click Start | Programs | Powertoys for Windows XP | TweakUI for Windows XP and expand the My Computer object in the left pane. Expand the AutoPlay object and then select Types. Clear the Enable Autoplay for CD and DVD drives check box (the Enable Autoplay for removable drives option is not selected by default).

Some third-party programs can temporarily store unencrypted (plain-text) passwords or other sensitive information in memory. Because of the Windows virtual memory architecture, this data can be present in the paging file. Therefore, you might want to clear the pagefile to increase the security of data while the computer is not running. To clear the pagefile at system shutdown, you must edit the Registry. Start Regedit.exe and navigate to HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management. Look for a data value of ClearPageFileAtShutdown. If it does not exist, you must add it as a type DWORD. Make the value 1. [21]

Prior to manually editing the registry, the recommended procedure is to make a backup of the data that you are going to edit. You can backup the whole registry, or just the key that you are modifying. In Windows XP, the newer version of the registry editor, Regedit.exe, is recommended for exporting registry keys. [22] You can backup a single registry key before modifying it; however, Windows XP encrypts some registry keys. You must be absolutely sure that the key does not contain encrypted values. Therefore, the safest method is to backup the whole registry rather than a single key. This is especially true if cannot ascertain if any data in the key you are modifying is encrypted or not.

To backup the registry in Windows XP Home Edition, you must use the Backup utility to backup the System State. The System State includes the registry, the COM+ Class Registration Database, and the boot files. The Backup utility will archive to another storage device, such as a hard disk or tape, however, the backup utility is not included in the default installation of Windows XP Home Edition. The program is included on the Windows XP installation CD-ROM in the ValueAdd folder and you can install it

manually. To install the Backup utility, double-click the Ntbackup.msi file in the *CD-ROM Drive*:\VALUEADD\MSFT\NTBACKUP folder.

I need to make a brief digression. One problem with using the Backup utility is that once it is installed, a user can access the Automated System Restore (ASR) wizard. The ASR feature is used on Windows XP Professional to enable users to create a set of floppy disks that can be used to automate the process of recovering a failed system. But, when you attempt to run the ASR Wizard on Windows XP Home Edition, you are likely to receive an error message and the operation is cancelled. Unfortunately, you do not always receive this error message and in that case you are allowed to create the startup floppy disks, which will not work in the event of disaster recovery. [23] Therefore, it is prudent to avoid using the ASR feature, even though it is accessible.

To backup the System State, click Start | All Programs | Accessories | System Tools | Backup. After the wizard starts, click Advanced Mode. Select the Backup tab and click New on the Job menu. Select the System State check box that is located under My Computer in the left pane. In the Backup destination list, click the destination that you want to use; you can backup to a file. Then click Start Backup.

When you backup the System State, NTBackup backs up the following registry hives: default, SAM, SECURITY, software, and SYSTEM. The location of the backed up registry files is \%windir%\Repair. [24] To recover the registry from a backup, you would boot to the Recovery Console and copy the computer's registry hives to \%windir%\System32\Config. To backup a single registry key, you would use the export command in Regedit.exe. Locate the key that you plan to edit and then on the File menu, click Export. In the Save in box, select a location to save the .reg file. In the File name box, type a file name and then click Save. If it turns out that you make a mistake editing the registry key and you want to return to the previous value, just double-click the .reg file that you saved.

Configuring Network Security

Many security guides mention that you should restrict anonymous logins to protect from Internet based attacks on your computer. In Windows XP Home Edition, anonymous login is restricted by default. The registry key HKLM\SYSTEM\CurrentControlSet\Control\Lsa\everyoneincludesanonymous controls whether permissions given to the built-in Everyone group apply to anonymous users. The default (value of 0) is that anonymous users do not have the permission of the Everyone group, which provides the same level of anonymous user restrictions as the RestrictAnonymous setting in previous Windows operating systems. (The Everyone group does not include the Anonymous Logon permission). [25] In addition, Windows XP HE prevents null session enumeration of logins. There is a registry key in HKLM\SYSTEM\CurrentControlSet\Control\Lsa\ named restrictanonymoussam. By default the value of this key is 1, which restricts anonymous enumeration of SAM accounts and names.

Likewise most security guides mention restricting remote access to the registry. On a Windows XP Home Edition-based computer, by default only members of the Administrators group can gain access to the registry over the network. If you desire to further restrict remote registry access, it is possible to edit a registry key. [26]

In order to reduce network-based security threats, many checklists stress the need to eliminate NetBIOS over TCP/IP, remove the Windows Client for Microsoft Networks, and prevent dynamic registration of IP address in DNS. I checked with Cox Communications and found that all three of the above configurations are required for my computer to successfully participate in their network. So, it is important to check with your ISP before following any of these standard recommendations.

However, one recommendation is to disable File and Printer Sharing for Microsoft Networks. This is actually the recommended setting from Cox Communications, so I am actually able to follow this recommendation on my Windows XP Home Edition computer.

You will also want to prevent anyone from using Remote Assistance to take control of your computer. To do so, open System in Control Panel. On the Remote tab, click the Advanced button. Clear the check box labeled Allow this computer to be controlled remotely.

When you run the Microsoft Baseline Security Analyzer you receive a report in which it is often suggested that you tighten security on Internet Explorer. This is accomplished by clicking Tools | Internet Options and selecting the Security tab. Make sure that the Internet Web content zone is selected and set the Security level for the zone to High.

The default privacy preferences in Internet Explorer 6 automatically restrict cookies that use your personal identifiable information for secondary purposes or to transfer such information to recipients beyond the site you are visiting. The default settings does allow for the collection of cookie data that is used for product delivery services. When the privacy icon appears in your status bar, this indicates that Internet Explorer 6 has taken a privacy protecting action on your behalf. Clicking on the icon brings up a privacy report that displays links to parts of the web page that can set or receive cookies. The report also indicates whether cookies have been blocked or restricted. This allows you to manage cookies on a site-by-site basis and accept or reject them as you feel appropriate. [27] Some of the options for managing cookies include: preventing all cookies from being stored on your computer; preventing third-party cookies, but allowing all other cookies; or allowing all cookies without notifying you.

Auditing Security Events

It is important to monitor the Security event log to make sure that there is no unauthorized activity on your system. In Windows XP Home Edition, you do not have the ability to configure your computer to audit user access to files, folder, and printers. However, you can manage the security events that are recorded by default.

Click Start and then right-click the My Computer menu option. Click Manage from the popup menu. Expand the Event Viewer object in the left pane and click on Security to view the security logs. The following events were found in my log: ID 512, 513, 514, 515, 518, 520, 528, 529, 538, 540, 551, 612, 615, 624, 626, 627, 628, 680, 682, and 683.

An explanation of the security events follows: 512 = system restart. 513 = system shutdown. 514 = authentication package loaded. 515 = trusted logon process registered. 518 = notification package was loaded. 520 = system time changed. 528 = user successfully logged onto a computer. 529 = logon attempt failed with unknown user name or bad password. 538 = user logged off. 540 = user successfully logged onto a computer (identical to 528). 551 = user initiated logoff. 612 = an audit policy was changed. 615 = an IPSec policy agent changed. 624 = user account created. 626 = user account enabled. 628 = user password set. 680 = logon attempt. From the extensive list of events recorded, including both successes and failures, it appears that the default setting on Windows XP Home Edition is to turn on security logging for both successes and failures.

To manage the Security log, click Start and right-click My Computer. Select Manage and then expand the Event Viewer object in the left pane. Right-click the Security log and select Properties. Set the log file size to something larger than the default (such as 2048 KB). You can leave the default setting of overwrite events as needed if you remember to save your event log on a regular basis. You can save the log file by right-clicking and selecting Save Log File As.

Set a regular schedule for monitoring the event log. You may want to use a basic third-party filtering and analysis tool such as NTLast by Foundstone. NTLast allows you to read saved event files, use date ranges in searches, and filter logons. [28]

System File Checker (SFC) is part of the Windows File Protection (WFP) feature that was introduced with Windows 2000. When a file in a protected folder is modified, the WFP feature is implemented. After the notification is received, the WFP looks up the file signature in a catalog file to determine if the new file is the correct version. If it is not, the file is replaced from the Dllcache folder or the installation source files. The WFP feature displays a dialog box to the Administrator when it performs the file replacement described above.

System File Checker allows you to manually scan all protected files to verify their versions. If SFC discovers that a protected file has been overwritten, it retrieves the correct version from a cache folder or the Windows installation source files and then replaces the incorrect file. SFC will also check and repopulate the cache folder. If the cache folder becomes damaged or unusable, you can use SFC to repair its contents.

So, if you suspect that your system has been compromised and you want to try to see if any system files have been replaced by malicious ones, you can use the sfc /scannow command. It will scan all protected system files immediately and replace incorrect

versions with correct Microsoft versions. This command may require access to your source Windows installation files.

Also, if you suspect that a file might be infected with a virus or has been compromised with malicious code, you can use the FC.EXE program to compare the file with a known clean backup copy of the file.

Fc.exe compares two files and displays the differences between them. For a comparison of a binary file, Fc reports the mismatched bytes from the two files. For a comparison of an ASCII file, Fc reports the lines from each file that differ.

Backups
To recover from a catastrophic malfunction that results in the need for total data recovery, the following process must be completed. First, manually reinstall Windows XP from the installation media. Second, install Ntbackup from the Valueadd folder on the installation CD-ROM. Finally, use Ntbackup to restore the data by using the backup set that had been created prior to the system failure. You must restore a full backup that includes the System State in order to carry out this procedure. The System State data includes: boot files, including the system files, files protected by Windows File Protection (WFP), the registry, performance counter configuration information, and the Component Services class registration database.

To backup the System State Data, click Start | All Programs | Accessories | System Tools | Backup. Then click the Advanced Mode. Select the Backup tab and then select the System State checkbox. Click Start Backup. Note: on my test, my System State backup used Shadow Copy to archive 2,098 files. The size of systemstate.bkf was 370 MB.

When you use the Ntbackup utility to make a backup of the data on your computer, volume shadow copy technology is used so that a computer can be backed up while applications and services are running. At the time a backup is initiated, an instant copy is made from the data and the backup is made from the shadow copy instead of the original volume. This means that files are not skipped during the backup process and the need for a scheduled backup window is eliminated.

Free disk space is used to a record of the differences between the original volume and the shadow copy volume. The data on the shadow copy volume only exists while the shadow copy is being taken. So, the amount of disk space temporarily used depends on how much data on the volume has changed during the backup. If sufficient temporary disk space is not available, the backup utility will skip open files. [29]

You cannot make a backup directly to a CD-R in Windows XP. Removable Storage Management does not recognize these devices as backup pool media. Therefore, if you want to copy a user's profile to a CD-R, you might want to backup to a file in the CD-Burning folder. The location of the CD-Burning folder is c:\documents and settings*user*

name\Local Settings\Application Data\Microsoft\CD Burning. That way it will be immediately ready to burn as soon as you insert the CD-R.

Summary

As you can see from the discussion above, Windows XP Home Edition lacks granular control over many aspects of its security, especially compared to XP Professional. For example, it is difficult to view file and folder permissions, the built-in Administrator account (Owner) is not exposed in the Welcome screen or in Control Panel, you cannot disable accounts that you create, and all accounts by default are placed in the local Administrators group. However, with a little time and effort, you can attain a much higher level of security than was possible in Windows 9x/ME. It is too bad, but understandable, that XP Home Edition does not implement many of the most important security features by default. Therefore, I would recommend that all certain actions be taken immediately. Use Windows Update and Automatic Updates to keep your system patched. Install the Microsoft Baseline Security Analyzer and follow its recommendations for securing your system. Change all user accounts but the built-in Administrator and the USERNAME account to limited accounts. Set a password on all users. Either use Internet Connection Firewall or a more robust firewall. Establish a TCP/IP port activity baseline. Install antivirus software and keep it up to date. Make regular backups of the System State and your user profiles to CD-Rs.

References

[1] “Microsoft Windows Update.” 2002. URL: http://v4.windowsupdate.microsoft.com/en/default.asp (10 Feb. 2003).

[2] “Microsoft Baseline Security Analyzer.” 2003. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/Tools/MBSAhome.asp (10 Feb. 2003).

[3] “Microsoft Baseline Security Analyzer (MBSA) Version 1.1 Q&A.” 9 Jan. 2003. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/Tools/mbsaqa.asp (5 Feb. 2003).

[4] “Frequently Asked Questions about the Microsoft Network Security Hotfix Checker (Hfnetchk.exe) Tool.” 11 Oct. 2002. URL: http://support.microsoft.com/default.aspx?scid=KB;en-us;q305385 (5 Feb. 2003).

[5] “Hotfix & Security Bulletin Service.” 2003. URL: http://www.microsoft.com/technet/security/current.asp (10 Feb. 2003).

[6] Thurrott, Paul. “Windows XP Home Edition vs. Professional Edition: What's the Difference?” 26 Nov. 2001. URL: http://www.winsupersite.com/showcase/windowsxp_home_pro.asp (5 Feb. 2003).

[7] Burnett, Mark. “Ten Windows Password Myths.” 7 Mar. 2002. URL: http://online.securityfocus.com/infocus/1554/ (10 Feb. 2003).

[8] “HOW TO: Set, View, Change, or Remove File and Folder Permissions in Windows XP.” 27 Oct. 2002. URL: http://support.microsoft.com/search/preview.aspx?scid=kb;en-us;Q308418 (5 Feb. 2003).

[9] “Jetico: Data Encryption Technology for Everyone.” 1995 – 2002. URL: http://www.jetico.com/bcwipe.htm (10 Feb. 2003).

[10] “Description of the Windows XP Internet Connection Firewall.” 18 April 2002. URL: http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B320855 (5 Feb. 2003).

[11] Wong, David. “Windows ICF: Can't Live With it, Can't Live Without it.” 22 Aug. 2002. URL: http://online.securityfocus.com/infocus/1620 (5 Feb. 2003).

[12] Wong, David. “Windows ICF: Can't Live With it, Can't Live Without it.” 22 Aug. 2002. URL: http://online.securityfocus.com/infocus/1620 (5 Feb. 2003).

[13] “ZoneAlarm 3.1.395.” 1995 – 2003. URL: http://download.com.com/3000-2092-10039884.html?part=zonealarm&subj=dlpage&tag=button (10 Feb. 2003).

[14] “Sam Spade.org.” ND. URL: http://samspade.org/ (10 Feb. 2003).

[15] Russinovich, Mark. “Process Explorer.” 2 Aug. 2002. URL: http://www.sysinternals.com/ntw2k/freeware/procexp.shtml (10 Feb. 2003).

[16] “Port Numbers.” 5 Feb. 2003. URL: http://www.iana.org/assignments/port-numbers (5 Feb. 2003).

[17] “Port Assignments for Commonly-Used Services.” Windows 2000 Resource Kits. 10 Oct. 1999. URL: http://www.microsoft.com/windows2000/techinfo/reskit/samplechapters/cnfc/cnfc_por_simw.asp (5 Feb. 2003).

[18] “What is SVCHOST.EXE?” 16 Oct. 2002. URL: http://www.igknighttec.com/Windows/WindowsXP/svchost_exe.php (5 Feb. 2003).

[19] “Windows XP Baseline Security Checklists.” 2001. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/xpcl.asp (5 Feb. 2003).

[20] “Microsoft Power Toys for Windows XP.” 23 Apr. 2002. URL: http://www.microsoft.com/windowsxp/pro/downloads/powertoys.asp (10 Feb. 2003).

[21] “How to Clear the Windows Paging File at Shutdown.” 11 June 2002. URL: http://support.microsoft.com/default.aspx?scid=kb;EN-US;314834 (5 Feb. 2003).

[22] “How to make a backup of the Windows Registry.” 2 Dec. 2002. URL: http://service1.symantec.com/SUPPORT/tsgeninfo.nsf/docid/199762382617 (5 Feb. 2003).

[23] “An Error Message Is Displayed When You Attempt to Use the Automated System Recovery Wizard.” 6 Aug. 2002. URL: http://support.microsoft.com/default.aspx?scid=kb;EN-US;302700 (5 Feb. 2003).

[24] “Windows XP System State Backup.” URL: http://www.jsifaq.com/SUBJ/tip4500/rh4595.htm (5 Feb. 2003).

[25] “HOW TO: Set, View, Change, or Remove File and Folder Permissions in Windows XP.” 27 Oct. 2002. URL: http://support.microsoft.com/search/preview.aspx?scid=kb;en-us;Q308418 (5 Feb. 2003).

[26] “How to Manage Remote Access to the Registry.” 11 June 2002. URL: http://support.microsoft.com/?kbid=314837 (5 Feb. 2003).

[27] “Overview of Internet Explorer 6 Privacy Features.” 7 Sep. 2001. URL: http://www.microsoft.com/windows/ie/evaluation/overview/privacyfeat.asp (5 Feb. 2003).

[28] “NTLast FAQ.” 2000. URL: http://www.foundstone.com/knowledge/proddesc/ntlast.html (5 Feb. 2003).

[29] “Volume Shadow Copy Technology.” 2003. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/winxppro/reskit/prdg_dsm_vtrj.asp (5 Feb. 2003).

Appendix A
A Security Checklist for Windows XP Home Edition

☐	Use Windows Update for manual security patching
☐	Configure Automatic Updates for scheduled security patching
☐	Run Microsoft Baseline Security Analyzer
☐	Change ordinary user accounts to limited type accounts
☐	Rename the local Administrator and Guest accounts
☐	Disable Welcome screen (optional)
☐	Require CTRL+ALT+DEL before login (optional)
☐	Verify that all partitions are formatted NTFS; use convert.exe if necessary
☐	Set a password on all user accounts
☐	Create private folders as needed
☐	Determine if a disk wiping utility is needed and implement if indicated
☐	Customize Windows Explorer's default view
☐	Activate Internet Connection Firewall (only cable modem and DSL users)
☐	Install ZoneAlarm (optional – for a more powerful personal firewall)
☐	Establish a TCP/IP port activity baseline
☐	Install antivirus software and schedule automatic updates
☐	Change the boot sequence to boot from hard drive only
☐	Install Tweak UI to make safe changes to the registry
☐	Disable Autoplay
☐	Clear the pagefile at system shutdown
☐	Backup the whole registry
☐	Further restrict remote access to the registry (optional)
☐	Disable file and printer sharing for Microsoft networks
☐	Disable Remote Assistance
☐	Tighten security in the Internet Zone in Internet Explorer
☐	Manage cookies on a site-by-site basis
☐	Regularly audit security events
☐	Use system file checker and fc.exe as indicated
☐	Backup the System State and profile folders regularly

Last Updated: July 22nd, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor