Interested in learning more about security?

SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Microsoft Windows XP Home Edition Security Implementation

This document is designed to guide home users on how to implement sufficient security measures on a home computer running Microsoft Windows XP Home Edition. It will provide you with loads of information to guide you to a more secure computing experience. This document contains no graphics in order to reduce the size of the document. There are plenty of tips and recommendations within this document to secure your environment sufficiently as well as possible spark your curiosity. The tools mentioned within this document ...

Copyright SANS Institute

Author Retains Full Rights

AD

Microsoft Windows XP Home Edition
Security Implementation

© SANS Institute 2003, Author retains full rights

Dennis Schrader
Version 1.4b Option 1
12/13/02

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Table of Contents

I. INTRODUCTION 4

II. PHYSICAL SECURITY 4

III. USER ACCOUNTS AND PASSWORDS 6

ADDING A NEW USER ACCOUNT 6
DISABLE / DELETE ACCOUNTS 7
ASSIGN STRONG PASSWORDS 7
SECURE THE ADMINISTRATOR ACCOUNT 9
SECURE GUEST ACCOUNT 9
PREVENT THE GUEST ACCOUNT FROM VIEWING EVENT LOGS 10
PASSWORD RESET DISK 10
MANAGING PASSWORDS 10
WELCOME SCREEN 11
WARNING MESSAGE 12

IV. FILE SYSTEMS 13

FILE SYSTEM 13
PRIVATE FOLDERS 14

V. KEEPING YOUR SYSTEM SECURE 14

PATCHES 14
SECURITY ALERTS 16
TESTING SECURITY SETTINGS 17

VI. FIREWALLS 18

INTERNET CONNECTION FIREWALL (ICF) 19
RESPONDING TO AN ATTACK 22
THIRD PARTY PERSONAL FIREWALLS 23

VII. ANTIVIRUS / VIRUS PROTECTION 25

FORMS OF THREATS 25
IDENTIFYING MALICIOUS SOFTWARE 26
INFORMATION SOURCES 27
PROTECTING YOUR COMPUTER 29
REPAIRING AN INFECTED SYSTEM 30

VIII. BACKUP AND RECOVERY 30

BACKUP METHOD 31
MEDIA TYPES 31
INTERIUM BACKUPS WITH WINDOWS BACKUP 33
BACKUP RECOMMENDATIONS 34
THIRD PARTY PRODUCTS 35
MISCELLANEOUS SITES 35
DISASTER RECOVERY 36

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

IX. SECURING INTERNET EXPLORER 36

SECURITY ZONE SETTINGS 36
ADDING A SITE TO A ZONE 37
CONFIGURATION 38
CONTENT ADVISOR 42

X. SERVICES AND PORTS 43

PORTS 43
ICF SETTINGS 45
TCP/IP FILTERING 45
IP SECURITY 46

XI. AUDITING 47

OTHER LOGS TO VIEW 47
THIRD PARTY TOOLS 48

XII. CONCLUSION 49

XIII. REFERENCES 50

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

I. Introduction

This document is designed to guide home users on how to implement sufficient security measures on a home computer running Microsoft Windows XP Home Edition. It will provide you with loads of information to guide you to a more secure computing experience. This document contains no graphics in order to reduce the size of the document. There are plenty of tips and recommendations within this document to secure your environment sufficiently as well as possible spark your curiosity. The tools mentioned within this document are to be used at your own risk and should be reviewed before installing them. You may get warnings from your AntiVirus software downloading some of the tools. I have found nothing wrong with the tools downloaded and installed on my system. Please enjoy this document and Welcome to Windows XP Security.

II. Physical Security

One of the most overlooked security measures is physical security. This happens to be the most important security feature to implement. If you keep sensitive data on your computer you need to ensure that only the people who need access to the data have access to the computer. If you are able to access the computer, you have the ability to possible access the data on that machine. "Physical security refers to the protection of building sites and equipment (and all information and software contained therein) from theft, vandalism, natural disaster, manmade catastrophes, and accidental damage (e.g., from electrical surges, extreme temperatures, and spilled coffee) as defined by the National Center for Education Services (NCES).[1]

There are a couple of things to consider for home computing. You need to require a login id and password for all users of the computer. This will prevent others from easily gaining access to your computer. It will also allow you to better track who does what on you computer as you will see in the auditing section of this document.

You also need to purchase a surge protector. A surge protector is a strip of outlets that you plug your equipment into to protect you from electrical surges. You can also look at purchasing a UPS (Uninterrupted Power Supply). This can be expensive and is usually not needed for home use. A UPS will allow your equipment to continue to run in the event that you lose power.

[1] Chapter 5, Protecting Your System: Physical Security, National Center for Education Services (NCES), http://nces.ed.gov/pubs98/safetech/chapter5.html

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

You need to ensure that all your cables, plugs, and other wires are out of the way of foot traffic. You can lose sensitive data if someone were to accidentally trip over your power source. This will help prevent a headache of having to restore your information or re-enter it.

You need to keep good track of you equipment. You need to record all of your serial numbers, manufacturing information, and other miscellaneous information about your equipment in a secure location. You might consider marking the outside of your equipment with paint, permanent marker, or something that is difficult to remove. This may reduce your re-sale value but will make it more difficult for a thief to covering their tracks in the event that your equipment is stolen. You should mark the inside of your equipment in the same manner. Again it makes it more difficult for the thief.

Another aspect of physical security to consider is the maintenance and repair of equipment. You need to ensure that your equipment is always in top condition in order to run it correctly. Ensure that it has adequate airflow to keep temperatures down, dust it regularly, and regularly use the equipment to ensure that it still functions properly.

When you step away from your computer you need to lock your screen. This will force you or another user to type in the password in order to use your login id on the machine. According to a Microsoft Article "A fast-typing attacker can get to your machine and share its disk drives with no passwords in under 10 seconds - but not if the machine's locked!"[2]

To do this with Microsoft Windows XP Home Edition you need to press your **Windows Logo Key** on your keyboard and the **L** key (**Windows Logo Key + L**). This will take you to the Welcome Screen if it is enabled (also known as Fast User Switching). Other users of the system will be able to logon with their login id and password to their account. You will be required to type in a password to resume your session. If the Welcome Screen is disabled then you will be presented with the **Unlock Computer** dialog box. You can also use the **On Resume, Use Welcome Screen** option of your screen saver. Once your screen saver kicks in (it should set to between 5 and 10 minutes) you will be brought to the Welcome Screen upon resuming your session. This will force you to type in a password.

Again physical security is one of the most important aspects of security. Physical access to a machine means that you have access to the data on the machine.

[2] 5-Minute Security Advisor - Basic Physical Security, Microsoft Corporation, http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/security/5min/5min-203.asp

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

III. User Accounts and Passwords

The next step to creating a secure environment is to create a logon id and password for all users on the system. This aspect may seem annoying for a typical home user but should be mandatory. It will slow a hacker or thief down for a while. This section is designed to guide you on how to manage user accounts and enforce strong passwords.

Adding a new user account

From the **Control Panel** select **User Accounts**. You will be presented with the User Account window. There are three tasks in this window that you can perform. 1**. Change an Account**. This will allow you to modify an account, change passwords for the account, change the user group for the account, and change the picture that is shown on the Welcome Screen. 2. **Create a New Account**. This is where you create new accounts and enter all the appropriate information that we will cover next. 3. **Change the way users log on and off**. With this option you can disable the Welcome Screen and disable Fast User Switching. Fast User Switching will allow you to log on with another account without logging off of your account first. Windows XP Home Edition makes it very easy to create a new account. Click the **Create a New Account** link to get started. You will be presented with a window instructing you to enter the name of the new account. This will be the user's logon id. Once you have entered the logon id for the user click the **Next** button. This will open another window. Here you will assign the account a type of privilege. There are only two types of access that can be granted in this window. Administration access will allow the use full access to all files and folders on the machine. This is the default group in Windows XP Home Edition. The other group is Limited. This access has limited privileges. With this type of access you can change or remove your password, change your picture, theme and other desktop settings; view files you create; view files in the shared folder; and users may not be able to install certain programs. There is a full description of the groups in the window. A user can only be assigned to one group using this method. Once you have decided on a group and have selected it you can press the **Create New Account** button. You will be returned to the User Account window.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Disable / Delete Accounts

Our next step is to disable or delete accounts that do not require access to the system. Disabling a user will prevent the user from logging on or accessing the system resources. The advantage of this method is that all the account information will not be deleted (SID, Private Files, Certificates, etc…). This means that when a user needs access again you only need to enable the account and the user will have all the files and personal settings as before. To disable an account you need to use command line options. From your start menu select command line. From the prompt you need to type **net user <username> /active:no**. Substitute the user's logon id for the <username> in the command. For more information on the net user command refer to Microsoft Knowledge Base Article - 251394.[3] If the command was successful you will get a confirmation from your command.

Deleting a user will prevent anyone from logging on with the account. This type of action is permanent. You will not be able to restore the user's access. Even if you create the user again with the same logon id it will be assigned a new SID. The user will not be able to access any of the information that they previously had (certificates, private folders, etc…). To perform this action, select the user that you want. You will be taken to another window with a link entitled **Delete User**. Once you select the **Delete User Option** you will be presented with two options. The first option is **Keep Files**. This will copy the user's files from their My Docs and Desktop to a file on your Desktop. You will have full control of the files. All their other items are deleted (e-mail messages, internet favorites, registry changes, etc…). The other option is **Delete Files**. This will delete all the user's files once you confirm this action.

Assign Strong Passwords

Now that we have created accounts for all our users and disabled users that don't need access we can assign strong passwords to all the users. There are two methods for performing this action. You can use the User Accounts window or you can use command line commands.

[3] Microsoft Knowledge Base Article - 251394 How to Use the Net User Command, Microsoft Corporation, http://support.microsoft.com/default.asp?scid=kb;en-us;251394&

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

User Accounts window can be opened from the **Control Panel**. Select the user that you want to add a password to. You will be presented with the Change Account window. Select the **Create A Password** link in the options list. This will open another window. On this window you need to enter the users password. You should keep these guidelines in mind. Passwords should be required for all users (at the very least the Administrator account needs a password). Passwords should be at least 8 characters long. Passwords can be up to 127 characters long. You should place both upper and lowercase letters in your password as well as at least 1 number and 1 special character (@,#,$,etc…). The password should not contain any part of the user's name or logon id. You should change your password at least every 90 days and the password should never be written down. There is an option to create a password hint. This is not recommended. It can be helpful to the user when they forget their password but all users can see it from the Welcome Screen as well. Once you have filled in the appropriate information click the **Create Password** button. You will be taken back to the Modify User screen. You will also notice under the user's picture it now says that it is password protected.

Using the command line options provides the same functionality as above. To get to the command line you need to open your **Start Menu -> Accessories -> Command Line**. Once you are at the command line prompt you need to type the following command.

net user <username> <password>

The username is the user's logon id or the name that appears on the Welcome Screen. The password has three options that can be used. 1. You can assign the user a password by typing the password that you want the user to have. 2. You can put a * there and it will allow the user to create their own **password (net user <username> *)**. 3. You can use **/random**. This will let the system randomly create a strong 8 character password (**net user <username> /random**). Any of these options are suitable. Once you have completed the information press **Enter**. You should get confirmation if your command was successful. If you selected the /random option it will present you with the password for the account. You need to inform the user of the password assigned.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Secure the Administrator Account

The administrator account is the most targeted account on systems. The administrator account has full access to the system and can perform all actions necessary that hackers are looking for. This account needs to have a very strong password. There are a couple of options to secure this account effectively. 1. You can change the name of the account. This will make it less obvious to hackers which account has full access. 2. You can create another administrator account and lock the default account and change it to limited access. This will temporarily trick the hacker. You still need to ensure that the account has a strong password. Your new account needs to avoid using logon ids such as god, admin, root, and administrator. These account names are not good at hiding the power of the account. Ensure that this account has a strong password as well.

Secure Guest Account

We now need to disable the guest account. This account has limited access to the system but if it is enabled if can be another option for entry to the system. Typically you will not have guests using your computer. If you do you can enable the account if they need access. From the **User Accounts** window select the Guest Account. You will be taken to the **Modify User** window. You should have a **Turn off the Guest Account** link. Click on the link and you will be returned to the User Accounts window. You will notice the under the Guest Account picture it states that the account is turned off. You may also want to remain the account for another layer of security. If the account is enabled, you need to open the command line and type **control userpasswords2** at the prompt. This will open a User Accounts window. On the **Users Tab** double click the Guest Account. You will get another window. On the **General Tab** type in a new name in the **Username** box. Once you have change the name you need to click **OK** to exit the edit. If you have no other accounts to change you need to click **OK** to exit the tool.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Prevent the Guest Account from Viewing Event Logs

Viewing the event logs could provide hackers with very valuable information about your system. You want to edit your registry. From the **Run** program in your **Start Menu**, type **regedit**. This will open your Registry Editor. You need to open **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog.** There are three groups located under **Eventlog**. You need to check all three groups (Application, System, and Security) to see if the DWORD **RestrictGuestAccess** is equal to 1. Below is a sample output.

RestrictGuestAccess REG_DWORD 0x00000001 (1)

This indicates that the **RestrictGuestAccess** is set to (1), which is restricted. (0) will allow the Guest Account access to the logs.

Password Reset Disk

The Password Reset Disk is used for users that have forgotten their passwords. Each user that wants to use this option needs to perform the following actions. Once you have logged on with the account that you want to create the disk for, you need to open the **Control Panel** and select **User Accounts**. There is a link entitled **Prevent a forgotten password** (starts a wizard). Once you have completed the wizard, store you disk in a secure location. If you need to use the disk to restore a password, from the Welcome Screen click **Use your password reset disk** or the **Reset** button if you are not using the Welcome Screen. You need to insert you disk and then choose a new password.

Managing Passwords

There are many ways to manage your passwords. You should not have one password that can be used for everything. You should have different passwords for different things. For example you should have 1 password to logon. That password should be used for nothing else. You should have a different password for secure sites and non-secure sites. You should have a different password for secure applications on your computer than your non-secure applications.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

You can keep your passwords in a text file. You should encrypt this file and save it to a disk. You need to save this disk away from the computer. This will allow you to write down your passwords with out having a paper copy of the passwords that is easily accessible. There are many Password Management tools located on the web. In your search engine type **"Password Management"**. You will get an enormous amount of sites that offer freeware, shareware, and purchased programs. One tool that I have found to be useful is **Password Corral**[4]. You can download this program from http://www.cygnusproductions.com/freeware/pc.asp. This tool stores the list of logon ids and passwords. You can encrypt the passwords and logon ids in this tool. You will password protect this tool so you are only required to remember 2 passwords (logon password and Password Corral Password).

Welcome Screen

While the Welcome Screen is convenient for users, it is a security risk. The Welcome Screen exposes user names and possible password hints for all the users on the system. You should consider disabling the screen so that the users need to use the Classic Windows Logon Window (**CTRL+ALT+DEL**). Disabling the Welcome Screen will disable the Fast User Switching as well.

To disable the Welcome Screen, from the **Control Panel** select **User Accounts**. Select the **Change the way users log on or off** link. This will open another window where you can clear the **Use the Welcome Screen** option. Click the **Apply Options** when you have completed your selections.

This can also be accomplished from the command line. Type **control userpasswords2** at the command line. This will open the **User Account Window**. On the **Advanced Tab**, there is a section at the bottom **entitled Secure Logon**. Select the option **Require Users to press CTRL+ATL+DEL**. Click **Apply**. Select the **Users Tab**. Up top there is an option to select entitled **Users must enter a login id and password to use this computer**. Then click **OK**.

[4] Password Corral V3.4.6.99, Cygnus Productions, David M. Fornalsky (Programmer), http://www.cygnusproductions.com/freeware/pc.asp

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

You also have the ability to hide certain accounts from being shown on the Welcome Screen if you still want to use the Welcome Screen. To do this you need to edit the registry. In the **Start Menu**, select the **Run** program and type regedit. This will open the Registry Editor. Change **HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\SpecialAccounts\UserList**. If you want to hide an account you need to change the DWORD to 0. An example of a hidden account is shown below

HelpAssistant REG_DWORD 0x00000000 (0)

If the DWORD is set to 1 then the user will be visible on the Welcome Screen. You can still logon to hidden accounts by pressing **CTRL+ALT+DEL** twice.

Warning Message

In recent years there have been many lawsuits that have been dismissed because the administrator did not display a warning message when you first logon. In order to make your system compliant for legal reasons you need to turn on a warning message when logging on.

You need to edit the registry using the **regedit** command in the **Run** program. You need to change the following **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon**. There are two options that need to change. **LegalNoticeCaption.** This will be the text that is displayed in the title bar of the logon window. The other option is **LegalNoticeText**. This will be the text that is displayed in the logon window.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

IV. File Systems

File System

Now that we have secured the user's login id, passwords, and have a physically secure computer we need to secure our file systems. The first step to this process is to convert your file system to NTFS (NT File System). Your system is probably already NTFS if you purchased it from another company (e.g., Gateway, Dell, etc…). You have the ability to check the file system type by clicking on **My Computer** (from your **Desktop** or **Start Menu**). Right-click on the icon for any drive (C:\). Choose **Properties** from the menu. Click on the **General Tab** of the **Properties** window. You will see the **File System** type located in the window (NTFS or FAT32). If the File System type is FAT32 or FAT you need to convert it to NTFS. From the command line (**Start Menu -> Accessories -> Command Line**) type **convert [volume] /fs:ntfs**. Since you are currently logged into the system you will get an error message. The message offers to convert the drive the next time the system is restarted. You want to say **Yes** to this option. You need to log off the machine and restart it. Converting the file system may cause some problems with permissions and the Master File Table (MFT) may become fragmented. Unfortunately the security benefit outweighs the risks with converting to NTFS. To circumvent the permissions issues you may want to consider using the **/nosecurity** option of the convert utility. This option specifies that the converted files and directory security settings are accessible by everyone. You have the ability to change the permissions later based on your needs. For more information on the convert utility you can go to the Microsoft Support Center.[5]

[5] Convert, Microsoft Corporation, http://www.microsoft.com/windowsxp/home/using/productdoc/en/default.asp?url=/windowsxp/home/using/productdoc/en/convert.asp

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Private Folders

The user also has options on how to secure files and folders within Windows XP. By default all folders and files in personal directories are accessible by all users in the administration group. For a user to lock out all the users, including the administrators group, they need to make their folder private. To use this option your file system has to be NTFS and the account must be password protected. By enabling this option the files or programs in your user profile and subfolders will be available to only you. From **My Computer** or **Explorer**, right-click on the folder that you wish to make private. On the **Sharing and Security Tab** select the **Make This Folder Private** option. You can also enable this option by going into **User Accounts** and removing (delete) and re-adding a password to the account. It will prompt you if you want to make your folder private. Select **Yes**. This option can not be granted on a file by file basis. There are ways around this but expert users who have experience with NTFS permissions should only perform them. In order to make the folders public again remove **the Make Folder Private** option or delete and re-add a password to the account.

V. Keeping Your system Secure

It is extremely important that once you get your system secure that you keep it secure. This section will deal with ways to keep your system secure. Some of the methods offered here range from patch installs, reading security alerts, and periodically testing your security levels.

Patches

Whenever there is a security problem or update a company will provide it's users a patch or hotfix to correct the issue and prevent other issues from arising. Windows XP has a way to automate this process for your Operating System and Microsoft tools. This tool is known as Windows Update. From your **Start Menu** select **All Programs**. There should be an icon entitled **Windows Update**. In order for Windows Update to work properly you need to be signed on as an Administrator. Once you open Windows Update you will be presented with a link entitled **Scan for Updates**. This program will scan your computer to reveal any updates that need to be updated. Based on the results of the scan the web site will provide you with three links (Critical Updates, Windows XP, and Driver Updates). If you have any updates that need to be downloaded and installed (as indicated by the web site) there will be a number next to each link. **The Critical Updates** are selected by default if there are any to download. Click on the link that you want to download and install. Click the **Review and Install Updates** link on the window. This will allow you to review the updates that Microsoft feels you need. You want to be sure to review all the changes that will be made. There are usually updates that you may not need to download or really don't need. For example, there may be a download to correct an issue with Microsoft

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Movie Maker. You never use this product, so why do you want to waste precious download time on this patch if it is not needed. Once you have selected the patches you want to download and install the process will begin. The download and install will walk you through everything that you need to do. Since Microsoft doesn't distribute updates on a regular basis, just on an as needed basis, you need to check the site often. Windows Update has a feature that will automate this process for you. With **Automatic Update** the Windows Update will check the web site for you to see if there are any patches or updates that need to be downloaded. Depending on the settings that you set you can have the Automatic Update download and install the fixes for you. By default Automatic Update will download the files but will not install them without your approval. Automatic Update will only retrieve critical updates so you still need to go to the site regularly to check for other updates. Once Automatic Update has downloaded an update a popup message will appear by the Automatic Update icon located in your **Start Title Bar** at the bottom. To configure Automatic Updates you need to open your **Control Panel** and select **System**. In this window is an **Automatic Updates Tab**. From this tab select **Keep My Computer Up To Date** checkbox. To disable this option, remove the check. There are three options to choose from when configuring the option. 1**. Notify me before downloading any updates and notify me again before installing them on my computer**. This is the best option for Dial-up users. This will allow you to approve all downloads so that you do not waste time downloading unwanted files. 2. **Download the updates automatically and notify me when they are ready to be installed**. This option is good for high-speed Internet users (DSL / Cable). Downloads will be automatic but you still have the ability to approve all installs. If you don't want a patch installed you don't need to. You still have the ability to install it another time if necessary. 3. **Automatically download the updates and install them on the schedule that I specify**. This option requires no user intervention. All the updates will be downloaded and installed without your knowledge or approval.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Security Alerts

Security alerts are emails or instant messages from companies, informing you of security risks or potential problems that are arising. These messages are usually sent the moment any issue has been confirmed, corrected, or informational. There are a couple different avenues you can pursue in this category. Microsoft comes with **Windows Messenger**[6]. In order to use this option you need to ensure that you are using Windows Messenger Version 4.5 or higher. If not, you can download Windows Messenger from http://messenger.microsoft.com/default.asp?client=0. Once it is installed you need to logon to Windows Messenger. From the **Menu** bar select **Tools**. There is a **Search for Contact** option. You need to search for updates that you want to receive. The web site will help you find what you are looking for. The moment a virus or security alert is issued you will see information in this window. This window will also offer links to their web site so that you can get more information.

Another option you have is to go to the particular web site for the product you wish to receive alerts from. Each site should have an option for **Net Alerts.** Net Alerts offer you a variety of ways to be notified of alerts (e-mail, instant message, pager, etc..). You will be notified the moment the company issues and alert so think about how you want to be notified.

There are several web sites that offer email alerts (usually free). Below are a few that I have found to be good. You can also perform a search on **"Security Alerts"** in a search browser to find more to suit your needs.

Microsoft Product Security Notification Services[7]

This is a free service provided by Microsoft. This service covers many Microsoft products and operating systems. You can register at the following address
http://register.microsoft.com/regsys/pic.asp

CERT Advisories[8]

This is another free services provide by the CERT organization. They are primarily responsible for Internet threats and responses. You can get more information for this service at
http://www.cert.org/contact_cert/certmaillist.html.

[6] Windows Messenger, Microsoft Corporation, http://messenger.microsoft.com/default.ashp?client=0
[7] Microsoft Product Security Notification Services, Microsoft Corporation, http://register.microsoft.com/regsys/pic.asp
[8] CERT Advisories, CERT Organization, http://www.cert.org/contact_cert/certmaillist.html

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

SANS Institute[9]

This is a free services provided by the SANS Organization. They work with different organizations to provide Administrators with one place to go to get information relating to security issues, vulnerabilities, and other helpful resources to complete your job at the highest level. You can pick which newsletters you would like to receive at http://www.sans.org/newlook/digests.

ZDNet [10]

ZDNet provides users with information on a broad range of topics. They evaluate equipment, offer free downloads, provide valuable resources, and provide security alerts. You can sign up for their service at http://nl.com.com/gen_login.jsp?brand=zdnet.

Testing Security Settings

To ensure that your security is working the way you expect it to you need to test it often. There are a number of utilities that you can use to perform these tests. No one tool is 100% effective so you should use a couple of them together. Each utility performs certain aspects of security checking. You need to check security vulnerabilities such as passwords, ports, viruses, Internet, etc… There are a number of free tools out there to help you perform these tests.

Microsoft Baseline Security Analyzer (MBSA)[11]

This will test your computer based on Microsoft Standards. You can obtain more information on system requirements and how to install it on the Microsoft web site (http://www.microsoft.com/downloads/details.aspx?FamilyID=e320cad4-6ac8-42e4-9f72-74d030ce7bd7&DisplayLang=en)

[9] SANS Institute, SANS Organization, http://www.sans.org/newlook/digests
[10] ZDNET, ZDNET, http://nl.com.com/gen_login.jsp?brand=zdnet
[11] Microsoft Baseline Security Analyzer (MBSA), Microsoft Corporation, http://www.microsoft.com/downloads/details.aspx?FamilyID=e320cad4-6ac8-42e4-9f72-74d030ce7bd7&DisplayLang=en

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Port Scanners

There are multiple port scanners available on the web. Port scanners will scan your ports and inform you of which ports are open and possible what is running on them or if they are listening. In your search engine search on **"Port Scanners"**. Here is one that I am using and have found to be good. SuperScan[12]. You can get this utility at http://packetstormsecuity.org/NT/scanners/superscan.exe. You need to type SuperScan in the search box.

John The Ripper[13]

John the Ripper is a password cracker. There are multiple versions of John the Ripper. You want to download the Win32 version of the cracker. You need to read the readme files for installation instructions and how to use this utility. John the Ripper is located at http://www.openwall.com/john.

Symantec Security Check[14]

This site offers multiple utilities to check your computer. They are free to use on a home computer. You can select which utility you want to use at http://security1.norton.com/ssc/home.asp?j=1&langid=us&venid=sym&plfid=21&pkj=IJBXVYRMHCGVRVRMNRY.

VI. Firewalls

Firewalls are programs or devices that provide barriers between a computer and the Internet. A firewall can be used between computers as well. Firewalls typically block traffic by performing packet filtering. The firewall will read the packets and determine, based on the rules you set, whether to let the packet in or not. Packet filtering happens by reading the Source IP Address, Destination IP Address, Network Protocol, Transport Protocol, Source Ports, or Destination Ports. The way the firewall filters packets is based on the rules that you set. You should have a firewall for any computer that connects to the Internet.

[12] SuperScan V3.0, Foundstone, Download package at PacketStorm http://packetstormsecurity.org/NT/scanners/superscan.exe
[13] John the Ripper, Openwall Project, http://www.openwall.com/john
[14] Symantec Security Check, Symantec, http://security.norton.com/ssc/home.asp?j=1&langid=us&venid=sym&plfid=21&pkj=IJBXVYRMHCGVRVRMNRY

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Internet Connection Firewall (ICF)

Internet Connection Firewall (ICF) is a firewall that comes packaged with Windows XP. Since this is a tool that you already have you should utilize it. From the **Control Panel**, open **Network Connections**. Right-click on the connection you want to protect. If you are using Dial-up it will be labeled **Dial-up Connection**. If you use DSL look for **LAN or High-Speed Connection**. From the menu select **Properties**. This will open the **Connection Properties** box. You want to modify the **Advanced Tab**. There is a check box located near the top that is entitled **Protect my computer and network by limiting or preventing access to this computer from the Internet**. To enable this option, place a check in the box. To disable, remove the check mark. Once you have enabled the option the **Settings** button will become available in the bottom of the window. This will allow you modify the settings for your firewall. There are three tabs on the **Advanced Settings** window (Services, Security Logging, and ICMP). On the **Services Tab** you have the ability to limit the services that are running on you computer from being used by Internet users. Some of the common ports that are used for incoming connections are listed below.

Service	Port	Protocol
FTP Server	21	TCP
Internet Mail Access Protocol Version 3 (IMAP3)	220	TCP
Internet Mail Access Protocol Version 4 (IMAP4)	143	TCP
Internet Mail Server (SMTP)	25	TCP
Post-Office Protocol Version (POP3)	110	TCP
Remote Desktop	3389	TCP
Secure Web Server	443	TCP
Telnet Server	23	TCP
Web Server (HTTP)	80	TCP

Windows Messenger uses the following services

Windows Messenger File Transfer	6891-6900	TCP

Uses one port for transfer. It opens 10 ports to allow 10 transfers at once.

Whiteboard and Application Sharing	1530	TCP

You can enable or disable any of these services that you like. You also have the ability to add more services by clicking on the **Add** button. Keep in mind that if you disable some of these services some of your applications may have problems. The ICF only affects incoming traffic so you should have no problems sending out traffic.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

The next tab located in the **Advanced Settings** window is **Security Logging**. On this window you select the logging options for the firewall. There are only two options (Log Dropped Packets, Log Successful Connections). **The Log Dropped Packets** option will log all the packets that were dropped by the firewall. You want to log this so that you can determine whether the access was an attempted attack or legitimate connections that were denied. **The Log Successful Connections** will log all the packets that were able to connect to you computer. If you log these type of connections you will get a file that is quite large. It is not recommended that you enable this option for a long period of time. The default location for the file is **%SystemRoot%**. It is called **pfirewall.log**. This file can be difficult to read so you will probably want to import the file in **Excel**. The file is constantly being written to, so you will need to open the file in **Read Only** mode.

The last tab in this window is **ICMP Options**. ICMP is Internet Control Message Protocol. This protocol is used to communicate on the Internet. ICMP carries no data and can be used for scanning networks, redirecting traffic, and DoS (Denial of Service) attacks. ICF by default blocks most types of incoming and outgoing ICMP messages. You have the ability to change the options for ICMP messages. Below are the options and a brief description.

Allow Incoming Echo Request

This means that your computer will respond to a ping (echo) request. This option is used typically for troubleshooting and could be turned on.

Allow Incoming Timestamp Request

This option will allow your computer to acknowledge certain requests with a confirmation message that indicates the time the request was received.

Allow Incoming Mask Request

This option will allow your computer to listen for and respond to request for information about the network it is attached to.

Allow Incoming Router Request

This option will allow your computer to respond to requests for information about it's routing tables.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Allow Outgoing Destination Unreachable

This option will allow your computer to respond to an unsuccessful attempt to reach your computer or another computer on your network with an explanatory acknowledgement of the failure.

Allow Outgoing Source Quench

This option will allow your computer to send source quench messages from your computer. A Source Quench is sent when a site or computer is sending information faster than your computer can process it. Typically the information that it cannot handle is dropped and a message is sent to the sending source to re-send the information at a slower rate.

Allow Outgoing Parameter Problem

This option will allow your computer to report back information to the sending computer that they sent an incorrect header.

Allow Outgoing Time Exceeded

This option will allow your computer to report back to the sender that their time has exceeded based on the **Time to Live (TTL)** information in the packet that was sent.

Allow Redirect

This option will allow your computer to respond to a request to redirect data to a different gateway.

Enable the options that best fit your situation. Once you have made all the option choices that you wish to make on the tabs, click the **OK** button at the bottom of the window. This will put all of your options in place and enable the ICF protection.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Responding to an Attack

Based on the information that you have gathered from your firewall log and you have determined that you have been attacked, there are a couple of options that you have in responding to the attack. You will want to notify your **Internet Service Provider (ISP)**. Provide them with all the details of the attack as you know them (who, what, where, when, and how). If you don't want to contact your ISP then you can contact **Dshield.org**[15] (http://www.dshield.org). Dshield.org is an organization that tracks reports of intrusions. You need to submit them all the information that you have concerning this attack. You will also need to send them your log showing that the attack occurred. They will analyze the reports that you submit and depending on the results that may contact the user's (attackers) ISP. If none of these seem like options you can go to the **NIPC** web site (www.nipc.gov/incident/incident.htm)[16]. NIPC (National Infrastructure Protection Center) is a division of the FBI. This site provides you with information on how to handle the attack. They have documents covering how to protect evidence, and how to help Federal, State, and Local Law Enforcement Agencies investigate the incident.

There are some general recommendations that you should follow. The first is to respond quickly. The longer you wait to report an incident the more difficult it can become to trace the attack. You should not stop any system processes or tamper with files. You may inadvertently destroy evidence on how the attack happened or who initiated the attack. You should use your telephone for all communications. If you have been attacked there is a chance that your e-mail has been compromised. By using e-mail you could have all your e-mails logged by the attacker or spread the attack to other computers and users. You will want to make copies of all the files that an intruder may have altered or left. This will help investigators determine how, when, and who initiated the attack. You should never contact the attacker yourself. You do not want to let them know that you know who they are. You could place yourself and your family in danger by contacting the intruder.

[15] Dshield.org, Euclidian Consulting, http://www.dshield.org
[16] National Infrastructure Protection Center, Division of FBI, http://www.nipc.gov/incident/incident.htm

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Third Party Personal Firewalls

If you are not satisfied with the options or abilities offered by ICF, you can find multiple utilities on the web. There are some free utilities that offer more options but are limited. If you purchase a firewall you will get most of the options that you desire. Below are some of the best known firewalls and sites.

BlackICE[17]

Internet Security Systems, Inc produces BlackICE. This is a purchased product located at http://www.iss.net/products_services/hsoffice_protection.

Firewall, Personal Firewall Plus[18]

Both of these utilities are produced by McAfee.com and need to be purchased. You can get information on these products and purchase them at http://www.mcafee.com/myapps/default.asp.

Norton Internet Security, Norton Personal Firewall[19]

These utilities are produced by Symantec Corporation and need to be purchase in order to use them. You can get more information on these products and purchase them at http://www.symantec.com/product/index_homecomp.html.

[17] BlackICE, Internet Security Systems, Inc., http://www.iss.net/products_services/hsoffice_protection
[18] Firewall & Personal Firewall, McAfee.com (A Division of Network Associates), http://www.mcafee.com/myapps/default.asp
[19] Norton Internet Security & Norton Personal Firewall, Symantec, http://www.symantec.com/product/index_homecomp.html

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

ZoneAlarm, ZoneAlarm Pro[20]

Zone Labs, Inc produces these utilities. ZoneAlarm Pro is a purchased product but ZoneAlarm is free. You get more features and enhancements with ZoneAlarm. You can get more information on both of these products and purchase Pro at http://www.zonelabs.com/store/application;JSESSIONID_ZL_STORE_COMMERCE=96HrF7uUdv2R0osgUUmt8lryokQI6AHoDddxMnGuMT1NjoF8YVlf!-1103240017!173109957!7511!7512?namespace=zls_main&origin=global.jsp&event=link.catalogHome&&zl_catalog_view_id=201.

Tiny Personal Firewall[21]

This is a purchased product as well. It is produced by Tiny Software, Inc. You can get more information as well as purchase this product at http://www.tinysoftware.com.

Utility Search Engine[22]

I have found this site to be useful to find freeware and shareware products. http://www.webattack.com. You can find several free firewalls here at http://www.webattack.com/freeware/security/fwfirewall.shtml.

Remember that any computer that is connected to the Internet should have a firewall protecting it.

[20] ZoneAlarm & ZoneAlarm Pro, Zone Labs Inc., http://www.zonelabs.com/store/application;JSESSIONID_ZL_STORE_COMMERCE=96HrF7uUdv2R0osgUUmt8lryokQI6AHoDddxMnGuMT1NjoF8YVlf!-1103240017!173109957!7511!7512?namespace=zls_main&origin=global.jsp&event=link.catalogHome&&zl_catalog_view_id=201

[21] Tiny Personal Firewall, Tiny Software, Inc., http://www.tinysoftware.com

[22] Webattack, http://www.webattack.com

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

VII. Antivirus / Virus Protection

As most people are aware there are many different forms of viruses in the world currently exploiting security holes, erasing data, or gathering information off of other people's computers. This section will deal with definition of treats, how to protect yourself, and how to repair you system in the event you get infected.

Forms of Threats

There are 4 basic types of threats. The first threat is from **Viruses**. Most people are familiar with viruses. A virus is a piece of code that replicates by attaching itself to another object (program, file, etc…). It usually happens without the user's knowledge. Viruses typically infect program files, documents, and low-level disk and file system structures. Viruses usually run when an infected program file gets executed. They can also reside in memory and infect files as the user opens, saves, or creates files. Viruses have the ability to change registry values, replace system files, and take over e-mail programs in order to replicate itself to other users.

Worms are independent programs that replicate themselves by copying themselves from one computer to another. This can be accomplished over networks or e-mail attachments. Worms have distributed most virulent outbreaks of hostile software in recent years. Many of these threats contain hostile code that can destroy data sites or launch DoS (Denial of Service) attacks against other computers. Viruses and worms are very closely related.

Trojan Horses are programs that run without the victims' knowledge or consent and are often disguised as other programs. This type of threat can be harmless. They are often used to perform functions that compromise the security of the computer by exploiting your access rights and privileges. Trojan horses can arrive via e-mail attachments or you can download them from a web site thinking it was a joke or software utility. This type of threat relies on basic social engineering to get users to install the malicious software.

The last threat is known as **Blended Threats**. These type of threats combine many characteristics of Viruses, Worms, and Trojan Horses. These type of treats often target web servers and networks. Unfortunately, this type of attack causes code to spread quickly and with extensive damage.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Identifying malicious software

There are some ways that you can identify that you have malicious software running on your server. You notice that there is a sudden burst of disk activity occurring. If you notice this happening, you need to open your Task Manager (**CTRL+SHIFT+ESC**). You want to click on the **Processes Tab**. This will display all the active processes that are currently running on your system. The **CPU** column will show you what percent of your CPU is in use by each application. By double clicking on the CPU heading it will sort the list in descending order. Find a process that is taking up a lot of CPU. Identify this program first, don't automatically assume that it is hostile. To identify the process you need to write the name of the process down. Using a Windows Search Utility, search for the program on your machine. Once you have found the program, right-click on it to display it's **Properties**. The **Version Tab** of the property window will give you product information. If the service is listed as **svchost.exe**, it is a program that is responsible for running a Windows Service. You can type **tasklist /scv** at a command line prompt. This command will list all of the Window's services running.

You may experience a sudden system slowdown. Viruses and Trojan Horses use a lot of system resources and can make your applications very slow. As stated before there may be a logical reason for the slowdown but you want to investigate it anyway. You can use the same process as before to identify the program that is slowing your system down.

You may have some unexpected network traffic. This may be legitimate programs running using Internet connects to get downloads. This also may be a threat that is using the network to spread to other users. The threat may also be using your computer for file transfers, keyboard logging, and DoS attacks. You need to identify the source of the traffic by reviewing your firewall and antivirus logs.

You may notice that some files have changed in size or have been renamed. This may be caused due to a threat that put new code in place or attached itself to the end of a program. You may notice extension changes (.doc to .doc.txt). This type of change is difficult to notice just by looking through your file listings. You need to use your backups to identify any changes in files or extensions. Most of your antivirus and firewall programs will notify you of these changes.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Information Sources

Due to the amount of threats that occur daily you need to have a couple of places to go to get up to date information on active threats. Below are some sites that I have found useful for information.

TruSecure Corporation[23]

This web site will provide you with current threats and hypes. There are multiple lists that you can look at on this site that list threats based on your needs. The web site listed next will take you to the Hype or Hot site. This site lists the current hype and hot threats http://www.trusecure.com/knowledge/hypeorhot/index.shtml.

CERT Coordination Center[24]

Carnegie Mellon Software Engineering Institute maintains this web site. It offers a list of vulnerabilities, incidents, and fixes. There are many links from this page to other areas of interest concerning security-related topics. The following link will take you to the Vulnerabilities, Incidents, & Fixes web page http://www.cert.org/nav/index_red.html.

Symantec Corporation[25]

Symantec Corporation is the producers of products like Norton AntiVirus and Norton Internet Security. This web site presents the list of threats, advisories, and removal tools. If you have a Symantec Product for Virus checking you will be able to download the Virus definitions from this page. http://www.sarc.com

Network Associates (McAfee)[26]

The link indicated below will take you to Network Associates Virus Information Library. Here they have a list of known viruses and hoaxes, how you can get infected, how they infect your system, and how to remedy the infection. http://vil.nai.com/vil/default.asp

[23] TruSecure Corporation, http://www.trusecure.com/knowledge/hypeorhot/index.shtml
[24] CERT Coordination Center, CERT Organization, http://www.cert.org/nav/index_red.html
[25] Symantec Corporation, http://www.sarc.com
[26] Network Associates Virus Information Library, Network Associates (McAfee), http://vil.nai.com/vil/default.asp

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Hoax Information

These sites provide information on virus hoaxes.

Symantec Corporation[27]

This web site will provide you with hoax information on a number of hoax viruses and e-mail letters.
http://www.symantec.com/avcenter/hoax.html

F-Secure[28]

This web site provides you with the latest hoaxes and false alerts. There are other areas of interest on this web site that you might want to check out. http://www.f-secure.com/virus-info/hoax/

Network Associates (McAfee)[29]

This web site is maintained by McAfee Security (a Division of Network Associates) and lists various hoaxes and false alerts.
http://vil.mcafee.com/hoax.asp

TruSecure Corporation[30]

ICSA Labs (a division of TruSecure Corporation) maintain this web site. This site offers multiple hoaxes and links to other helpful areas of security.
http://www.icsalabs.com/html/communities/antivirus/hoaxes.shtml

[27] Symantec Corporation, http:/symantec.com/avcenter/hoax.html
[28] F-Secure, http://www.f-secure.com/virus-info/hoax
[29] McAfee Security, McAfee (a Division of Network Associates), http://vil.mcafee.com/hoax.asp
[30] ICSA Labs, ICSA Labs (a Division of TruSecure Corporation), http://www.icsalabs.com/html/communities/antivirus/hoaxes.shtml

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Protecting your computer

There are a couple of things you can do to protect your computer. Each one of the items listed below are important and you should consider putting them in place on your computer. The first thing you should do is install an AntiVirus Software. The installation usually occurs in two phases. The first phase consists of installing the scanning engine. The scanning engine is the code that is used to check your machine for viruses or holes. The next thing to occur is the installation of the virus definitions. The virus definition is a database that contains virus signatures that are used to identify certain threats. The next phase to the installation is to update the software to the latest version of the virus definitions. You can usually set this up for automatic updates within the utility. If you cannot you need to update the database at least once a week.

The next step you can take to protect you computer is to ensure that your system is up to date. This means that your AntiVirus Software is updated and you have installed all the patches, hotfixes, etc… on your computer.

You need to ensure that your e-mail program is setup to block dangerous attachments that arrive via email. You can configure what to block out in Outlook Express and Outlook. You should also check you AntiVirus software application. They typically have options to filter e-mail messages. You can also check with your ISP to see how to install or use these options in their application.

You need to install a firewall program. You can use the ICF program that is available in Windows XP. It will stop unwanted intruders. It cannot stop programs from sending data from your computer though. You need to get a firewall that has 2 way (incoming, outgoing) protection. The firewall will help you identify Trojan Horse programs and some have the capability to detect Spyware.

The last thing you can do to protect your system is to backup your data regularly. This can save you a big headache if you ever needed to recovery your system after an infection.

An important thing to remember is that AntiVirus Software is not 100%. The software is limited to known attacks, meaning that it cannot pick up undetected viruses. AntiVirus Software is a reactive process. The company will first identify the virus. This consists of tearing the virus apart, adding it to a signature file, and then making the signature file available to the public. During this process your computer is vulnerable to the new virus. AntiVirus Software can also provide you with false positives. This means the computer will indicate that a file is infected when you know for a fact that it is perfectly safe.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

If you do receive an alert, you need to investigate it every time. The alerts may provide you with the name of the virus. What you can do is go to the companies web site and get more information on the virus. It may tell you ways to clean up the virus and how to protect yourself for the future. If the alert suggests a heuristic scan, this means that the file doesn't match any virus in the signature file. This may be a perfectly acceptable file but you need to investigate to ensure that it is not corrupt or hiding any information. If you are still unsure on the warning you can contact the vender and send them the file so that they can investigate it themselves.

Repairing an infected system

If you feel that your system has been infected you need to perform some tasks to repair it. The first thing you need to do is to positively identify the infection. You do not want to restore a system or waste needless hours to find out that you really were not infected to begin with. If you have identified that you are infected, you need to isolate the infected computer. This means if you are connected to the Internet or a network than you pull the plug on the network or modem. Once you have done that you need to get the proper tools or utilities to clean your system. Some companies provide cleanup tools on their web site to assist you in your recovery process. A good collection of tools can be obtained for the Symantec Corporation[31] web site located at http://www.sarc.com/avcenter/tools.list.html. If there are no tools are available, then you will need to delete all the infected files and replace them with your backup copies. In extreme cases of infection you will need to reformat the disk, re-install your Operating System, restore all the applications, restore all your data from clean backups, re-install your antivirus software, and scan other computers on your network. As you can see it is extremely important to protect yourself from the beginning so that you are not forced to perform an extreme recovery case.

VIII. Backup and Recovery

As shown in previous sections backups are extremely important even in a home environment. Most users do not think to backup their data. They either feel that they won't crash or be infected, or that it is for corporations and companies only. This section will provide you with backup methods, media types, and some utilities.

[31] Symantec Corporation, http://www.symantec.com

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Backup Method

There are two different backup categories that can be used. **Normal Backups** are full backups of all selected files. When a **Full Backup** occurs the files archive attribute will be cleared. The file archive attribute notifies the backup utility if a file has been created or changed since the last backup. This will prevent other backup types from backing up data that has not changed since the last backup. The next category for backups is **Interim Backups**. This category is used in between your Normal (Full) backups. There is different Interim Backup types. You need to choose which type best suites your situation. The first type is **Incremental**. This type of back will copy files that have changed or been created since the last normal or incremental backup. It will clear the archive attribute once the file has been backed up. The next type is **Differential**. This option will copy the files that have been changed or been created since the last normal or incremental backup as well. The difference between incremental and differential is that differential does not clear the archive attribute. The next type of back up is **Copy**. This will copy the files that you select. This does not remove the archive attribute from the file. This type of backup can be used a way to archive a particular file without changing your backup routine. The last type of backup is a **Daily Backup**. This backup method will copy all the files that changed or were created on the current day. This does not remove the archive attribute. This can be used to backup a particular day's work without changing your backup routine. This method is not recommended though. The problem with this method is that any files that are changed after a backup is run are missed and won't be picked up on the next daily run. For example, if you run your daily backup at 10:00 and you change a file at 11:00 P.M. This file will not be backed up. The next run at 10:00 P.M the next day will only backup from 12:00 A.M. to 10:00 P.M. that day. Another problem with this backup method is that if you miss a day for any reason your files will not be backed up for that day.

Media Types

Once you have determined a backup method, you need to decide on the media type to use for storage. There are many options that can be used. There are good points and bad points for each method.

<u>Floppy Disk</u>

As a backup method this is not a good type to use. Most floppy disks hold around 1.44 MB of memory. If you performed a full backup you would need several hundred disks in order to fit your whole system on them.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

High-capacity Floppy Disk

This type is good for interim backups. A typical zip disk can hold about 100 MB - 250 MB worth of data. A JAZ disk can hold anywhere from 1 GB - 2 GB worth of data. The downside to this method is that it is expensive and to slow for full backups.

Tape

This has been the media choice traditionally. Most corporations use tape for backups. The problem with tape backup is that it is slow for full backups and it must be attended to.

Hard Disk

This method is the most convenient. You will need to have a partition or another machine with enough space to store you backup. This method can be run unattended so that it can be done while you are away or sleeping and won't interfere with your computing needs.

CDR / CD-RW

This is the least expensive backup media. It is used primarily for long-term archival storage. The drawback with this media type is that it typically holds about 650 MB worth of data. This can mean that you need a couple disks to perform a full backup.

DVD

This media type can hold around 9.4 GB per disk. The drawback is that currently DVD / RW are a bit pricey.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Interim Backups with Windows Backup

Windows Backup is a utility that comes with Windows XP. This utility will perform most of you backup needs. It unfortunately can not perform partition backups. You can start this utility by using your **Start Menu** or command line. From your **Start Menu** select **Programs -> Accessories -> System Tools -> Backup**. If you prefer the command line you can type **ntbackup**. **The Backup or Restore Wizard** will open. Click on the **Backup Tab**. If you prefer to specify your own backup parameters you need to click on the **Advanced Mode** link. You now need to select the folders that contain the data that you want to backup. In the **Backup Media or Filename** box type in the name of the file or your backup partition that you will place your backup data on. Choose **Job**. This will save your backup job definitions. Click **Start Backup**. In the **Backup Job Information** box you need to make some selections. You need to type the description of the backup job in the appropriate box. You want to select the **Replace** option so that your backup job creates a new file with the same name each time you run it. You should also select the **Allow** checkbox. This will ensure that only the administrators group has the ability to restore files from you backup. Now select the schedule you would like your backup to run on. You are required to enter your password and click **OK** before you get to the scheduling options. Your backup can run at anytime because Windows Backup runs without interrupting your work. Once your job has completed you will want to compress the file using a zip utility. This will make the file smaller and it can usually fit on one disk. You will be able to password protect the file and **winzip** will allow you to span across multiple disks if necessary. If your file is larger than 4 GB then you will not be able to use winzip. In this case you need to modify your backup job so that it creates two or more files.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Backup Recommendations

Backups can take up a lot of space and can be expensive unless you streamline your process. This section will show you tips on how to reduce the size of your backup and possible speed the process up. The first thing you will want to do is to delete files you will never need. Why should you back them up regularly if you are never going to use them. You can save it to a disk and delete it from your system. The next step is to uninstall programs that you no longer use. Programs can take up a lot of space and will add more time and space to your backup. This will help your system in multiple ways, it will free up space on your computer that can be used for other things, it will require less space for backup, your backup could run faster, and there will be less to recovery in the event that you need to. Once you have completed those steps you will want to run the Disk Cleanup utility. The Disk Cleanup tool helps you free up space on your hard disk by searching your disk for files that you can safely delete. You can choose to delete some or all of the files. Use Disk Cleanup to perform any of the following tasks to free up space on your hard disk. Remove temporary Internet files, remove downloaded program files, empty the Recycle Bin, remove Windows temporary files, remove optional Windows components that you are not using, and remove installed programs that you no longer use. You can run this program by right clicking on the drive that you want to clean in explorer. Choose **Properties** and choose **Disk Cleanup**. You can also access this utility by typing **cleanmgr** at a command line prompt. The next step you can perform will be to reduce the space allocated to the Recycle Bin. Right-click on the **Recycle Bin** and choose **Properties** to complete this. On the **Global Tab** there is a slider that will reduce the amount of space allocated. You might also want to consider reducing the size of your Temporary Internet Files cache. From **Internet Explorer** select **Tools -> Internet Options** from the **Menu Bar**. On the **General Tab**, click on the **Temporary Internet File Settings** button. Again there is a slider that can be moved to the left to reduce the cache. If you have Hibernation enabled you should consider disabling it. **Hibernation** is a Power Management option that saves and image of your computer's RAM on your drive before shutting down. When you turn the power back on you will be booted where you left off. You can disable this option through your **Control Panel -> Power Options**. There is a **Hibernation Tab** and you need to clear the box **Enable Hibernation**. The next step to consider is to enable your computer to delete the **Page File** on shutdown. The Page File is a large file that is used as virtual memory. In order to change this setting you will need to edit the registry by using **regedit**. Under **HKLM\System\CurrentControlSet\Control\SessionManager\MemoryManagement** there is an option entitled **ClearPageFileAtShutdown**. This option needs to be set to 1 to enable it. Setting the option to 0 will disable the option. If you have a partition that you don't back up you should consider moving your page file to that partition. Right-click on **My Computer** and choose **Properties**. On the **Advanced Tab**, click on the **Performance** button. Click on the **Advanced Tab**

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

and click **Change**. Select the drive and set the size of the page file. The last thing you should consider is to reduce the amount of space allocated for **System Restore**. This is a feature that saves restore points and lets you restore your system files to a previous point in time if necessary. To adjust this setting right-click on **My Computer** and choose **Properties**. Click the **System Restore Tab** and select the drive that you want to change and adjust the slider for **Disk Space Usage** box. These tips should help you reduce the size and speed of your backup strategy.

Third Party Products

There are many products out there that you can purchase or download to provide you with another backup utility. The utilities can give you more options and features that you might want to create a sounder backup plan.

Drive Image[32]

Drive Image is a product that is used to quickly create backup hard drive images. Power Quest Corporation produces it. This is a purchased product. You can get more information or purchase the product at their web site shown below.
http://www.powerquest.com/driveimage

Norton Ghost[33]

Symantec Corporation produces this product. This is a product that can be purchased. You can get more information or purchase the product at their web site shown below.
http://www.symantec.com/sabu/ghost/ghost_personal

Miscellaneous Sites

Below are some sites that can help you find software.

Lexun Freeware[34]

This site offers tools to enhance you XP experience. There are some tools here for backup and recovery.
http://home.carolina.rr.com/lexunfreeware

[32] Drive Image, Power Quest Corporation, http://www.powerquest.com
[33] Norton Ghost, Symantec Corporation, http://www.symantec.com
[34] Lexun Freeware, http://home.carolina.rr.com/lexunfreeware

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

WebAttack.com[35]

This site features utilities, software, and programs to help you. They offer shareware and freeware. You can perform a search in the site to find backup and recovery utilities.
http://www.webattack.com

Disaster Recovery

Disaster Recovery is a process that you hope you never have to use. Depending on which utility you choose will dictate how your recovery process will work. I encourage you to learn how the process works and periodically test the process. This will help ensure that you understand what your product or utility will do for you. It will also give you an idea of how long it would take to restore your system. You can adjust your strategy once a test is completed, so that it works without a hitch, in the event that a real disaster occurs.

IX. Securing Internet Explorer

Windows default Internet program is **Internet Explorer**. If you have an ISP you are probably using another browser to surf the Internet. This section will deal with users that are using Internet Explorer. It will cover how to set security zone settings and configure the **Content Advisor**. You want to make sure that all the latest patches, rollups, and hotfixes are applied. These should be current if you are using **Windows Update** and the **Microsoft Security Notification Service** as mentioned in previous sections.

Security Zone Settings

Security Zone Settings are settings that you can configure for specific zones (local intranet, trusted sites, restricted sites, and internet). **The Local Intranet Zone** is used to secure sites within your organization / network. These sites are located behind a firewall and you usually have a high-level of trust with these sites. The **Trusted Sites Zone** is a site that is located outside your firewall. These are sites that you have a high-level of trust with. They may be companies that you typically deal with or trust (e.g., Microsoft, Gateway, Dell, or other Users that you trust). The **Restricted Sites Zone** is for site that you do not trust. This site is empty by default. The **Internet Zone** is for any site that does not fit in another category. All of these zones are configurable by the administrator of the machine.

[35] WebAttack.com, http://www.webattack.com

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Adding a site to a zone

If you have found a site that you trust or want to restrict access to, you need to add the site to the zone. In order to accomplish this you need to first select the zone that you want to add the site to. There is a button entitled **Sites** that you need to click **Next**. This will open another window. In this window you need to either type or paste the URL information of the site. If you are adding a site to the Local Intranet you need to click on the **Advanced** button to put in the URL information. By entering the full path, you will in effect add the whole site. For example I want to trust the following web page http://www.microsoft.com/windowsxp. By entering the whole URL I have actually trusted the whole site http://www.microsoft.com. If a site has the URL of http://ftp.microsoft.com/, this site will not be trusted based on the rule I created earlier. You need to ensure that what you are adding is really what you want added. This is an all or nothing situation. If you are using DNS names or IP Addresses to access site then you need to add both the DNS name and IP address to the zone in order for the settings to be effective. There is an option box that will **Require server verification (HTTPS:)** for all sites in this zone. This option will ensure that the site you are currently entering is secured with SSL. You can have both secure and non-secure sites in the same zone. If you are entering a non-secure zone then you need to make sure that this option is not selected.

If you need to move a site from one zone to another (trusted to restricted) you need to follow the next steps. First you need to delete the site from the original zone. Internet Explorer will not allow duplicate entries. Once you have deleted it from the other zone you are able to add it to the new zone.

One thing you need to do is to check your zones frequently. Some programs that you install will actually update these zones and add sites. If you no longer want a site there or find a site that was added and shouldn't be, you need to delete it from the list by pressing the **Remove** button.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Configuration

You have the option to change the default settings for each zone. Below are the settings and a brief description of the settings. The Local Intranet is defaulted to **Medium-Low** security, Trusted Sites are at a **Low** security setting, Restricted Sites are at a **High** security setting, and the Internet is at a **Medium** setting.

Once you have selected the zone you want to change the settings on click on **Custom Level** to configure the settings yourself.

Active X Settings

Download signed Active X Controls
This option allows your computer to download controls that can be assumed to be authentic and unaltered. If option only downloads without a prompt from you trusted sites by default. You want to consider changing this option to Prompt because you can not guarantee a signature from anyone.

Download unsigned Active X Controls
This option allows your computer to block unsigned Active X controls without a prompt. All zones are set to Prompt for this type of request by default. This option is at a good level and you should not need to modify it.

Initialize and Script Active X Controls not marks as safe
This option determines whether to allow initialization and / or scripting of Active X Controls that do not have the appropriate "safe for" signature. The default selection for this option is suitable for home use.

Run Active X Controls and Plug-ins
This option allows the running of downloaded Active X controls and Plug-ins. The default setting in all the sites except Restricted is to do this without a prompt. For Restricted sites you want to make sure that it is set to Disable.

Script Active X Controls marked safe for scripting
This option determines whether controls loaded with the <parm> tag are allowed to interact with scripts. This option is enabled in all zones except Restricted.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Download Settings

File and font downloads are enabled for all the zones except Restricted. As long as you have an Up-to-Date virus checker this default is reasonable.

Java Settings

There are 5 settings that can be performed in this section. You can set the level at custom**, Disable Java, High Safety, Low Safety, Medium Safety**. If you set it to **Low Safety** and a download that is signed with corresponding permissions request can become comparable in power to Active X. If you set the level higher you will still be able to run programs but you will be prompted if you have not granted them enough power.

Miscellaneous Settings

Access Data Sources across domains
This option determines whether a component that needs to connect to a data source is allowed to connect to a domain other than the one from which it was downloaded. This option is not permitted by default in the Internet or Restricted Zones

Allow Meta-refresh
This option will redirect a user to another site if it has moved after a specified delay. If this option is disabled you will not automatically be forwarded to the new site but will need to copy the forwarding address in the address bar.

Display Mixed Content
This option determines what the browser should do when it encounters a site that wants to display both secure and non-secure content. By default in all zones it is set to Prompt you. You want to be careful on these types of sites because you do not know what is secure and what isn't.

Don't prompt for client certificate select when no certificate or only one certificate exists.
This option determines what the browser should do when a web site requests a certificate. By default this is disabled in all zones. If you have only one certificate that is trusted at the site you can enable this setting to avoid being prompted. If you have more than one certificate per site Internet Explorer will display a list of certificates that you can use.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Drag and Drop or Copy and Past Files
This option is enabled by default for Local and Trusted Sites. The issue with having this enabled is that a file could potentially have a script or control to move from a restricted site to a lower security site where it can do what it wants. Unless you are 100% confident in your Trusted or Local Site you should consider changing this to **Prompt**.

Installation of desktop items
This option is enabled by default only in the Trusted zone. This option allows you to protect yourself against a security vulnerability that could allow a user to gain unauthorized privileges on your computer.

Launching programs and files in an IFrame
IFrames are in-line, floating frames that are often used for pop-up windows. Some security problems related to IFrames have been buffer overflows and hostile scripts. This option is enabled by default only in the Trusted zone.

Software Channel Permissions
This option controls the permissions given to software distribution channels. There are three levels that this option can be set at. **High Safety**. This option will prevent you from being notified about software updates by e-mail and keeps software from being automatically downloaded and installed. **Medium Safety**. This option will allow you to receive e-mails and downloads as long as they are digitally signed. There is no automatic installation with this option. **Low Safety**. This option will allow you to receive e-mail notification and will automatically download and install the software.

Submit non-encrypted form data
This option affects the transmission of forms data over non-SSL connections. You can have this option Disabled, Enabled, or Prompt. Disabling this option will disable the transmissions, Enabling this option will allow the transmissions, and Prompting will prompt you to see if you want to perform this or not.

Userdata Persistence
This option allows web sites to create XML files that store personal data for reuse by the web site. This is enabled in all the zones except Restricted. This is not a security risk because you choose what information to provide to the web site.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Scripting Security Settings

Active Scripting
This option determines whether scripts are allowed to run on web pages. This option is enabled by default on all zones except Restricted sites.

Allow Past Operations via Script
This option allows scripts (under certain conditions) to copy data from the user's clipboard to the host web site. This option is enabled in all the zones except Restricted. You should consider changing this option to Prompt or Disable.

Scripting of Java Applets
This option determines whether scripts are allowed to interact with Java applets. This option is enabled by default in all the zones except Restricted.

User Authentication Settings

This option determines what to do if a web site requests your logon. As a general rule you should not allow automatic logon anywhere except (possibly) in Local and Trusted Sites. The reason is that a malicious web site operator could log all of the information and then crack your password over time.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Content Advisor

The **Content Advisor** is a feature that will block web pages from being displayed based on settings you setup. The users can still access the pages if they enter the Supervisor password.

Internet Explorer uses a rating system to block sites. The rating system is known as **RSACi** (Recreational Software Advisory Councils internet)[36]. There is another rating system that you should consider downloading. The Internet Content Rating Association (ICRA) produces this system[37]. To configure Content Advisor you need to first download the ratings file for the ICRA. The ratings file and other information on how to install and set it up are located at http://www.icra.org/_en/faq/contentadvisor/. Once you have installed the ratings file you can now setup your content filter. The ICRA rating file gives you a lot more categories to filter than the RSCAi (4 categories). For each category there is a number associated. This number indicates the explicit or intense rating. The number range from 0 - 4 and the higher the number the more explicit or intense the content.

You need to select the categories you want to filter and then set the limit for them. A description of the current setting will appear under the slider as you move it so that you can choose the appropriate setting. This step must be performed for each category that you want to implement. Once you have made all your settings you need to click **OK**. You will be prompted to type in a Supervisor password. This password will be used to override the filter if you wish to view a web site that has been disabled.

Not all sites are rated. For these types of sites you will get a dialog box to instruct Internet Explorer on what to do. You have three options for the site. You can **always allow the web site to be viewed**, **always allow this web page to be viewed**, or you can **allow viewing only this time**. Whatever option you select you will be required to type in the Supervisor password. If you don't want to protect your computer that you way you can set it so that all users can see sites that have no rating. To do this you need to open Internet Options and go to the **Content Tab**. There is a **Settings** button on this page. Click the **Settings** button. There should be a **General Tab** in this box. On that page there is the setting **Users can see sites with no ratings**.

[36] RSACi, Recreational Software Advisory Councils Internet, http://www.rasc.org (no longer a valid organization. They folded into the ICRA).
[37] ICRA, Internet Content Rating Association, http://www.icra.org

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

You also have the ability to create your own ratings for a particular site. On the **Approved Sites Tab** in the **Content Advisor** you can type the URL of each site. You can select whether to always approve the site or never approve the site. The one thing that is bad about the Content Advisor is that it controls all users not just one account.

To disable Content Advisor you need to select the **Disable** button on the **Content Tab** of **Internet Options**. You will be required to enter your supervisor password.

X. Services and Ports

Services and ports are security risks that you can only minimize and not eliminate. This section will focus on how to secure your services and ports to minimize the risk of intrusion.

Ports

A port is not a physical port but an arbitrary number that 2 computers agree upon to identify each other's communication channel. There are two types of communication primarily used on the Internet. The first type is **TCP**. This stands for Transmission Control Protocol. It is a long lasting connection between two computers to ensure messaged is received reliably. With TCP if a connection is lost or corrupted the transmitting computer and the receiving computer will try to re-establish the connection to retransmit the data. The next transmission type is **UDP**. UDP stands for User Datagram Protocol. This is a low overhead protocol. UDP is a one packet simple message. If the connection is lost neither computer will try to re-establish it. UDP is used for streaming media or video.

The Internet Assigned Numbers Authority (**IANA**)[38] is responsible for assigning port number from 1 – 1023. These port numbers are well known. They also coordinate the registration of port numbers from 1024 – 49151. Port numbers 49152 – 65535 are not managed and are used by each application differently. You can get a list of registered ports from the IANA web site located at http://www.iana.org/assignments/port-numbers. Port numbers are used so that a user can talk to an application. Applications listen on certain ports. When you invoke an application you are having the application connect to the designated port.

[38] IANA, Internet Assigned Number Authority, http://www.iana.org

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

You need to periodically check your active ports. You can use multiple tools to investigate ports. First tool you want to use is the **Task Manger**. You can open this tool by pressing **CTRL+SHIFT+ESC**. You should click on the **Processes Tab**. You want to make sure that the **Show Processes from all users** box is selected. You have the option to sort this window by any column that you wish. You need to click on the column header of the column that you want to sort by. In XP you need to add the PID column. The PID is the Process ID of the process that is running. From the **View** option in the **Menu Bar** use the **Select Columns** option. This will open another window that you can select which columns you want to add. Select **PID** and click **OK**. If you find a process that you don't recognize you can run the Tasklist command at the command line. Once you are at a command prompt type **tasklist /svc**. This will list the names of all the windows services that are running along with the PID and image listing of the service. Another command that you can use to help investigate is the netstat command. From the command line, type **netstat -an**. This will list display the current protocol statistics and current connections. There are five columns in this output. The first column is the **Protocol** (TCP or UDP), then **Local Address**, **Foreign Address**, **State**, and **PID**. Your computer has three different local addresses (0.0.0.0, 127.0.0.1, and 10.0.0.3). After each IP address is the port number that the address is connected to or listening on. A Local Address output sample is 0.0.0.0:135. The IP address is 0.0.0.0 and the Port number is 135. Below is a sample line from the netstat command.

TCP 0.0.0.0:135 0.0.0.0:0 LISTENING 944

TCP is the protocol for this output. The Local Address is 0.0.0.0 (your IP) and the port number is 135. The Foreign Address is 0.0.0.0 (your IP) and the port number is 0. This service is currently in a **LISTENING** state. This means that the port is open and waiting for another computer to connect to it. Another state that a port can be in is **ESTABLISHED**, meaning that the port is currently talking to another computer. The PID of this service is 944.

Now that we have most of the information necessary to investigate the service, we need to check with the IANA port list to see what service or application uses port number 135. Next you want to check the Task Manager to see what service has the PID of 944. If the service is listed as **svchost.exe** you can use the tasklist command next to get a name of the service. You now can determine whether you should leave this port open or close it.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

There are three methods that can be used to restrict access to ports. The first tool is **ICF** (Internet Connection Firewall). This tool can be configures to block all incoming traffic except for response to communications initiated by your computer. This will prevent hackers from trying to access ports that might be listening. The next is **TCP/IP Filters**. These are used to permit or deny requests based on IP address, port number, or protocol for both your computer and remote computers. Experienced administrators who need to allow incoming traffic to listening ports typically use these tools. The last tool is **IP Security** (IPSec). This tool is similar to TCP/IP filters except that it provides the ability to secure traffic with encryption and authentication. Extremely knowledgeable administrators who want to allow incoming traffic while protecting against hackers who might be eavesdropping use this tool.

ICF Settings

ICF settings were covered in an earlier section of this document. Please refer to this section to get more details on how to setup ICF.

TCP/IP Filtering

From the **Control Panel** select **Network Connections**. Right-click on the **Local Area Network** and choose **Properties**. On the **General Tab select Internet Protocol (TCP/IP)**. Click the **Advanced Button** and select the **Options Tab**. Select **TCP/IP Filtering** and then **Properties**. In the TCP/IP Filtering window check the **Enable TCP/IP Filtering (All Adapters)**. There are three sections that you will need to configure (TCP Ports, UDP Ports, and IP Protocols). There are 2 options for each section. **Permit all** will allow all packets through**. Permit Only** allows you to enter the port or protocol numbers that you want to allow. All other ports and protocols will be closed for that section. This utility will only monitor incoming traffic. Be sure to only open ports that you want remote computers to access. This method of filtering is not very effective and is hard to configure. You have more control over types and methods of filtering if you use ICF.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

IP Security

All network activity uses IP by default. This tool will monitor both incoming and outgoing traffic. It can also recognize specific IP traffic. You have the option of blocking, permitting, or permitting traffic after securing it with authentication, encryption, or both. IP Security negotiates a security association between computers commonly known as **End-to-End Security**. Due to the complexity of this setup you should refer to the Microsoft Documentation[39] referenced below for more information and how to setup this utility.

http://search.microsoft.com/default.asp?IntCat=0&Boolean=ALL&Nq=new&qu=IPSec&finish=Go&ig=1&siteid=us/products/windows/windowsxp

Unfortunately blocking ports is not enough. Even carefully firewalled networks can be porous to a wide variety of services. Also, outgoing web traffic is rarely blocked. To help secure the computer even further, you need to minimize the amount of software that is run on the system. You should only have essential services and applications running. All other services or applications should be disabled or stopped.

Services

Services are programs that run continuously in the background, processing request from other programs on the network. Typically users rarely interact with the services directly. By shutting down services that aren't needed your security will improve as well as your system performance. There are a couple of ways to view the services that are running on your system. From the **Control Panel** select **Administrative Tools** (under **Performance and Maintenance** Category if in category view). You can also type **services.msc** at the command. Once you are in the **Service Console** there will be a list of all the services running on the system. Services that are running have a **STARTED** in the status field. The **Startup Type** indicates how the service is started and when it gets started. There are three types of Startup Methods. The first is **Automatic**, which means the service starts when Windows boots. **Manual** will start when a program requests the feature that the service provides. **Disable** will never start.

[39] Microsoft Documentation, Microsoft Corporation, http://www.microsoft.com

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

To turn a services off you need to change the Startup Type. You should first consider stopping the services manually without changing the Startup Type. Run the computer for a while and see if any problems arise. If a problem does arise you can start the service again to see if the problem is corrected. If you find a service running that you have previously stopped these means that another program has requested the use of this services. This service should not be considered for turning off. If your computer has run a couple of days with no problems you can change the Startup Type. I would suggest changing it to **Manual** so that if another program does need access to this service down the road you won't have a problem. If you decide to switch it to **Disable** then you need to remember that the service will never get started. This will apply to critical programs and operations as well.

XI. Auditing

Auditing and monitoring allow you to track activity of users and security sensitive changes to the system. Windows XP Home Edition does not have great auditing tools by default. It does come with an Event Viewer that can be access from the **Computer Management** option under **System Tools** in the **Control Panel**. Click on **Administrative Tools** and then **Event Viewer**. From the command line you can access this utility by typing **eventvwr.msc**. You have the ability to view the **Application Logs**, **Security Logs**, and **System Logs**. Next to each incident there is either a **Key** (successful attempt) or a **Lock** (failed attempt). You can double click on the even to get more information on the event. By default each log file has a maximum size of 512 KB. This can be adjusted up or down in 64 KB increments. Each file has a life of 7 days by default. To adjust the properties you need to right-click on the log file and choose **Properties**. If the log is unable to add new events to the log because you told it to never overwrite or if fills up before the logs have reached their life timeout, you will receive a warning. To correct this issue you need to clear the log or archive and clear the log.

Other logs to view

ICF generates a log that should be reviewed periodically as well. This file by default is located in **%SystemRoot%\pfirewall.log**. This is a text file and would probably be easier to view in **Excel**. If you have another Firewall or AntiVirus Software installed, you need to review the logs generated by them as well. You need to consult the instructions for the programs to find out where the logs are stored and what changes can be made to them.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Third Party Tools

Below are a couple of tools that can assist you in auditing your system.

http://www.foundstone.com/knowledge/free_tools.html[40]

This site offers tools that cover assessment, forensics, intrusion detection, scanning and stress test. You can download one or all the tools. They are easy to use and can be very helpful. They are free for home use.

http://windump.polito.it/install/default.htm[41]

This site offers versions of windump. Windump is a utility that can sniff packets for windows. This is a free tool for home use.

http://www.nmapwin.org [42]

This site offers nmap versions for windows operating systems. Nmap is a port scanning utility. This is a free tool for home use.

http://www.openwall.com/john[43]

This site offers a password cracker called John the Ripper. You need to ensure that you download the right version (Windows vs. Unix). This is a free tool for home use.

http://www.ethereal.com/distribution/win32/ethereal-setup-0.9.8.exe[44]

This site offers the Ethereal product. Ethereal is a network and packet sniffing utility. This is a free tool for home use.

http://www.pcmag.com/article2/0,4149,137188,00.asp [45]

This article offers you the opportunity to download a utility called Startup cop. Startup Cop is a tool used to create startup profiles in Windows.

[40] FoundStone, http://www.foundstone.com
[41] Windump, Windump: TCPdump for Windows, http://windump.polito.it
[42] nmap, Sourceforge.net, http://www.nmapwin.org
[43] John the Ripper, Openwall Project, http://www.openwall.com
[44] Ethereal, http://www.ethereal.com
[45] PC Magazine, http://www.pcmag.com

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

http://www.jpsoft.dk/download.html[46]

This site offers LPS. LPS is a utility that is used to scan your computer for open / listening ports. This is a free tool for home use.

http://www.webattack.com/get/regmon.shtml[47]

This web page allows you to download regmon. Regmon is a utility that is used to monitor changes to your registry. This is a free tool for home use.

http://www.sysinternals.com/ntw2k/utilities.shtml[48]

This site offers system utilities for Windows environments. You can download filemon V4.34 here. Filemon is a utility that monitors all of your files. This is a free tool for home use.

http://www.webattack.com/freeware/network/fwnetmoni.shtml[49]

This web page lists a variety of different network monitoring tools. TCPView will show you a detailed listing of all TCP and UDP endpoints on your system. This is a free tool for home use.

http://www.webattack.com/freeware/security/fwpass.shtml[50]

this web page lists a variety of different password management tools. Whisper 32 is a password tool that allows you to store encrypted passwords and also has a password generator. This is a free tool for home use.

XII. Conclusion

There was a lot of information presented in here and you may feel overwhelmed. Do not fear security. Security is an ever-changing process that needs to be played with and tweaked to stay on top. I hope that this document has sparked your interest in security and has given you a stepping point to thinking in a more secure manner concerning your computer and data. Fortunately there are plenty of articles and documentation concerning Microsoft Windows XP. Good Luck.

[46] LPS (Local Port Scanner), JPSoft DK, http://www.jpsoft.dk
[47] WebAttack.com, http://www.webattack.com
[48] Filemon V4.34, SysInternals, Mark Russinovich and Bryce Cogswell, http://www.sysinternals.com
[49] WebAttack.com, http://www.webattack.com
[50] WebAttack.com, http://www.webattack.com

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

XIII. References

National Center for Education Services (NCES)
http://nces.ed.gov/
(As of 12/13/02)

Microsoft Corporation
http://www.microsoft.com/
(As of 12/13/02)

Cygnus Productions
http://www.cygnusproductions.com/
(As of 12/13/02)

CERT Organization
http://www.cert.org/
(As of 12/13/02)

SANS Organization
http://www.sans.org/
(As of 12/13/02)

ZDNET
http://www.zdnet.com/
(As of 12/13/02)

FoundStone
http://www.foundstone.com
(As of 12/13/02)

Openwall Project
http://www.openwall.com
(As of 12/13/02)

Symantec Corporation
http://www.symantec.com
(As of 12/13/02)

Dshield.org
http://www.dshield.org
(As of 12/13/02)

SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

National Infrastructure Protection Center (NIPC)
http://www.nipc.gov
(As of 12/13/02)

Internet Security Systems, Inc.
http://www.iss.net
(As of 12/13/02)

McAfee.com
http://www.mcafee.com
(As of 12/13/02)

Zone Labs, Inc.
http://www.zonelabs.com
(As of 12/13/02)

Tiny Software, Inc.
http://www.tinysoftware.com
(As of 12/13/02)

Webattack.com
http://www.webattack.com
(As of 12/13/02)

TruSecure Corporation
http://www.trusecure.com
(As of 12/13/02)

F-Secure
http://www.f-secure.com
(As of 12/13/02)

ICSA Labs
http://www.icsalabs.com
(As of 12/13/02)

Power Quest Corporation
http://www.powerquest.com
(As of 12/13/02)

Lexun Freeware
http://home.carolina.rr.com/lexunfreeware
(As of 12/13/02)

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Recreational Software Advisory Councils Internet (RSACi)
No longer a valid organization. They folded in with the Internet Content Rating Association (ICRA)
http://www.rasc.org
(As of 12/13/02)

Internet Content Rating Association (ICRA)
http://www.icra.org
(As of 12/13/02)

Internet Assigned Number Authority (IANA)
http://www.iana.org
(As of 12/13/02)

Windump: TCPdump for Windows
http://windump.polito.it
(As of 12/13/02)

nmap
http://www.nmapwin.org
(As of 12/13/02)

Ethereal
http://www.ethereal.com
(As of 12/13/02)

PC Magazine
http://www.pcmag.com
(As of 12/13/02)

JPSoft DK
Http://www.jpsoft.dk
(As of 12/13/02)

SysInternals
http://www.sysinternals.com
(As of 12/13/02)

Microsoft Windows Security Inside Out for Windows XP and Windows 2000
Ed Bott and Carl Siechert
Microsoft Press
Copyright 2003

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

GSEC Security Essentials Toolkit
Eric Cole, Mathew Newfield, and John M. Millican
Que Publishing
Copyright 2002

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: June 19th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**