Global Information Assurance Certification Paper

A Best Practices Guide

To

Secure a Windows® XP Professional Installation

Zacharias Groves
GSEC Practical Assignment
v.1.4b – Option 1

Table of Contents

Abstract

Securing a workstation is more artistic and abstract than it is an exact science. It takes time and practice to get just the right fit for each environment. The Windows® XP Professional operating system is a workstation operating system meant for business use. As a result of being created for business use, it was created with security in mind. Despite being created with security features and tools, when installed with the default options there are many features which make the operating system not secure. Leaving the operating system unsecured by default is done with the intent to help maintain compatibility and ease of use with applications that will later be installed on the operating system. This document is meant to be a recommendation guide to help outline important features in the operating system enabling you to create a stronger level of security to your Windows® XP Professional installation. This document will not cover domain level technologies, such as Active Directory. Domain level security features may be used in conjunction the security technologies proposed in this guide. As a result of Windows® XP Professional being built on Windows NT technology many of the security settings recommended from Windows® NT and Windows® 2000 still apply, for information on securing Windows 2000 Professional see "Building a Secure Windows 2000 Professional Network Installation" by Bruce Fyfe in the SANS' Reading Room. This document will focus on the Windows® XP Professional operating system and its enhanced security features. Please recognize the fact that this is just a recommendation guide. The settings in this guide may not be appropriate for your particular circumstance and may cause your machine and applications to stop working. It is recommended that before using each and any of these recommendations that you backup or image your configuration.

This guide will be exploring the security concepts of "Defense in Depth", "Confidentiality, Integrity, and Authenticity" (C-I-A), and the "Principle of Least Privilege". "Defense in Depth" is a layered approach to security in which the key goal is to maintain Information Assurance (IA). The layered approach reaches to all levels of the information process, including: Personal / Physical Security, Device Security, Network Security, Perimeter Security, and Application Security. Information Assurance is achieved through the security services of Confidentiality, Integrity, Authentication, Availability, and Non-Repudiation[i]. These security services or principles complement each other to help individual assess threats and to maintain the integrity of their digital communication from start to finish. The "Principle of Least Privilege" establishes that users are only given the access to the information, devices, and applications that are necessary to perform their daily functions within an organization. The three concepts, "Defense in Depth", "Confidentiality, Integrity, and Authenticity" (C-I-A), and the "Principle of Least Privilege", do complement and overlap one another. It is through these concepts that the suggestions outlined in this guide hope to make

your Windows XP Professional operating system as secure as possible to maintain the integrity of your data.

Physical Security

One of the most overlooked steps when attempting to achieve Information Assurance is physical access to a machine. If your computer is a laptop, a person may just walk off with it. The question then becomes not if they are going to gain access to information you did not want them too, the question is how long before they gain access to it, proving again it is no longer your machine. This is the best place to start to practice "Defense in Depth". If the room that the computer is in can easily be accessed then the computer may be easily compromised. Despite having a BIOS password, removal of the system board battery may be good enough to remove the password from memory[ii]. If your machine is left unattended, attackers can install key loggers and USB drives or smart cards containing root kits, viruses, and Trojan Horses. Installing these devices and malicious software, malware, will allow them to retrieve you passwords and your essential information. A precautionary suggestion is a workstation lock. These are actual cables that attach to your machine to a desk or wall so that the machine cannot be physically removed. This type of option is very necessary for laptops that can be easily picked up and put into an attacker's bag.

First, It is recommended that you make sure that the building and room that your machine or machines are located in can only be accessed by those authorized to be there. Second, authorized access to a building or room does not grant a person the authority to access the any or all machines. In order to maintain Least Privilege, you will want to utilized BIOS passwords, Hard Drive passwords, and some sort of two or three factor authentication for access to the operating system such as a USB token or smart card combined with a personal identification number, PIN, and a thumbprint scanner.

Another precautionary method to limit a person's access to the resources on your machine is to limit the boot order to hard drive only; this can be done in the BIOS. In order to limit availability, you may want to consider removing or disabling floppy, CD/DVD-ROM, CD±R/RW, and DVD±R/RW drives completely from the machine. This practice will limit information being added or taken away from the machine via this medium.

After installation you it would also be recommended to disable any Ethernet or Wireless network cards, Bluetooth and Infrared devices, USB, Smart Card, Serial, and Parallel ports. Disabling these devices in the operating system will limit their availability to an attacker. If you are plugged into an Ethernet network and your Wireless Network card has not been disabled, there is potential for an attacker to connect to your machine and use it as a router. Maybe the attacker

will not be successful in obtaining your data, but they may use your machine to attack someone else.

Perhaps you have a modem line attached to your computer. An attacker may be using a war-dialer to randomly access your modems and fax machines. Using a brute-force attack it is only a matter of time before they will be able to gain access.

Operating System Installation

Installation Media

When you install your base operating system to the machine, the safest way to install it is via an OEM or Retail CD. If it is from any other medium make sure that the operating system has been MD5 or SHA1 hashed so that you can verify that no one has tampered with it. For instance, if you have a network or other custom installation image an attacker have added root kits, malware, viruses, or Trojan Horses without your knowing it. If you take a hash of the installation, you have the ability compare it to the original checksum and verify the authenticity of all files. For the purposes of this paper it is recommended that you use a Retail or OEM CD from Microsoft, as to make sure that base OS has not been tampered with.

What not to install?

If you are not going to use them some options that you will want to remove from the base operating system include: MSN/Windows Messenger, MSN Explorer, Outlook Express, Internet Games, and Windows Media Player. These options will be installed into the base OS and can be removed by going to Add/Remove Programs. They are listed under Add/Remove Windows Components. If you are going to uses any or all of these components it is recommended that you have the latest versions and that they have been patched with the latest updates. You will find these updates on Microsoft's Windows Update site, but you may also want to go to the web page for each particular product and make sure that there are no updates that are newer.

During the installation process you will be asked for Network Settings. The settings here will depend upon the requirements for your internet connection, but it is recommended to statically enter the IP address of your machine. To limit the machines that are able to talk to your machine, limit the subnet by limiting the subnet mask. In a non-domain or non-workgroup environment it is recommended to remove the "Client for Microsoft Networks", "File and Printer Sharing for Microsoft Networks" , and "QoS Packet Scheduler". Removing the "Client for Microsoft Networks" and "File and Printer Sharing" will reduce the number of ports listening and the opportunity for your machine to respond back in a matter that will provide a challenge response authentication window from which an attacker to try to authenticate. These options can be found under the "Properties" for Internet Protocol (TCP/IP), click on the button labeled

"Advanced". On the DNS tab you will want to remove "Register this connection's address in DNS", unless you are attaching your machine to a domain. On the WINS tab you will want to uncheck "Enable LMHOSTS lookup" and check "Disable NetBIOS over TCP/IP". This will limit your machine from advertising itself via NetBIOS and listening for NetBIOS information. Remember to apply the recommended settings to each Network Card.

What to install?

In the initial stages of a fresh installation you will have to choose between NTFS or FAT32 as the file system on the hard drive. NTFS is the only recommended file system. NTFS allows you to assign security privileges and encrypt your data is why it is the only secure choice. It is also recommended that you use the entire drive and format it with NTFS. Using the entire drive removes the availability for another operating system to be loaded on to the machine. Loading another operating system may allow an attacker to bypass the security of your current installation. If you are upgrading to Windows XP Professional it is recommended to convert your drive to NTFS. The version of NTFS in Windows® XP does assign tighter security than Windows® 2000. Windows® XP does not assign the "Everyone" group with Full Control access, as in Windows® 2000. Never issue the "convert /fs:ntfs /Nosecurity" command. This command will assign the "Everyone" group to Full Control as was the default in Windows® 2000.

Another choice of preference to install with the base operating system is the Internet Connection Firewall. If you currently don't have firewall software or hardware firewall, the ICF is a recommended choice. It will give you basic firewall protection until you are able to purchase a third party firewall which will be discussed in a later section.

User Accounts

The default administrator account will be created on installation with the password that you set during the installation. Remember to use a complex password for the administrator account. You will then be asked to create at least one more account. It is recommended to create two additional accounts, one account with which you will administer the machine and one account that you will use on a daily basis with limited access. When creating the user accounts it is recommended to make sure that the names of neither of the newly created accounts are your email address. If your account name and email address are the same then the only thing an attacker needs is your password allowing a limited amount of time before your computer can be compromised by a brute force attack. You will not be asked for passwords for these accounts. You will have to set the passwords upon first login. Once you login you will have to navigate to the Control Panel > Administrative Tools > Computer Management > Local Users and Groups. If you do not see these options you may have to switch to the "Classic" View. You will now have to set your daily account to have limited access. You will have to set the passwords on both accounts as well as setting a

password for the Guest account. The default administrator and guest account should be disabled, because even if you rename the account it can be attacked by using the Security ID, SID, which is the same across all Windows® XP Professional machines. An additional suggestion is to remove the descriptions from the default Administrator and Guest accounts. You will be disabling both of these accounts, but removing the descriptions will add another layer of defense, we will be renaming both the accounts through the Local Security Policy later in the guide. You may take the opportunity to do it now. To make each user have to press the CTRL+ALT+DEL button, it is recommended to remove the "Fast User Switching" and the "Use Welcome screen" to login. Make a user have to physically depress the CTRL+ALT+DEL keys, limits the ability for an attacker to use a program to brute force an interactive/console logon.

New to Windows® XP are the two accounts for Remote Assistance. If you want to give Microsoft the ability to log into your machine to help you then you may want to keep these accounts, but disable them. Otherwise, I suggest deleting the "HelpAssistant" and the "SUPPORT_388945a0" accounts. If you do decide to remove these two accounts then you will also want to delete the group called "HelpServicesGroup".

Software Updates and Patches

After installing the base operating system, securing the user accounts, and removing the application features that you don't intend to use. The next step is to install software patches and updates. First, go to the Windows Update site to find all Critical and Recommended Updates and Service Packs for the operating system. You should not install Windows Media player or the .NET Framework if you are not going to use them. If you have installed any other software such a Microsoft Office it is recommended that you not only have installed the latest versions, but to also have gone to the software manufacturers website and download the latest hofixes, patches, and service packs for those as well.

After installing all of the patches to the operating system you will want to go back to the Add / Remove Programs Wizard and make sure that no new features were installed that you may not want. If you do not want to have Outlook Express or Windows Messenger installed you will need to verify it there. One feature that is installed after Service Pack 1 is the "Internet Gateway Device Discover and Control Client"[iii] , this client sends out traffic to try and find a gateway even though one may be specified in your IP address configuration. You should uninstall this client.

Post Installation Hardening

One key theme for the following settings will be to make sure that there will be no history kept of any documents or websites that you have been to. The purpose of erasing where you have been is to make it difficult for an attack to be able to trace any data that may compromise you any further. If an attacker is able to go to web pages that you have been to before they may be able to obtain your credit

card information, thus making a simple compromise of your machine a financial nightmare. These are further steps to ensure Confidentiality, Integrity, Authenticity, and Non-Repudiation.

Folder Options

One of the easies ways for you to be able to see viruses, malware, and Trojan Horses is to allow yourself to see hidden files and file extensions. In order to enable these features you will have to open the Folder Options console in the Control Panel.

View

- Check / Select:
  - "Display contents of system folders"
  - "Do not cache thumbnails"
  - "Show hidden files and folders"

Uncheck:

- "Hide extensions for know file types"
- "Hide Protected operating system files"
- "Remember each folder's view settings"

These settings are per user so they will have to be done for each user account that you have added to the computer. Allowing file extensions to be viewed will help to prevent such exploits as “kournikova.jpg.vbs”.

File Types

The Settings made in this section will have to be done to each user profile for which you want the desired settings to be applied.

While still in the Folder Options console, choose the File Types tab. In order to prevent viruses and malware from spreading throughout your registry and installing or moving itself throughout your computer you may want to files that end in *.JS, *.JSE, *.REG, *.VBE, and *.VBS to open with Notepad or Wordpad. This may cause problems with some OEM utilities from your computer manufacturer. OEM Manufacturers sometimes use Visual Basic Scripts in order to do maintenance tasks behind the scene.

Another way to stop the scripting files from being executed is to disable the Windows Scripting Host[iv] as described in SANS/FBI Top 20. This can be done with an application from Symantec called noscript.exe. This will help to prevent such attacks as those by the Love Letter Virus.

Offline Files

The setting made in this section will affect all users so will not have to be made under each user profile. If you are going to connect to a workgroup or domain then you will want to make sure that “Encrypt offline files” is checked. This will make sure that the data is protected and if it is a laptop the data will not be able to be retrieved unless someone is able to

authenticate as you. Also if you are going to use offline files it is best if you disable Hibernation Support, in the Control Panel > Power Settings. The hibernation temporary file is not able to be encrypted and your information will be able to be retrieved from it.

If you are not connected to a workgroup or domain and you are not going to use Offline files then uncheck "Enable offline files".

System Properties

The following steps can be changed from the Group Policy level, but you will want to disable them from this level also, that way if there are problems with the policy loading then the desired settings are still set.

Advanced

Under the “Startup and Recovery” heading there is a “Settings” button. You should click the “Settings” button. Under the “Write Debugging Information” heading you should change the option to “none”. The debugging information can contain pieces of your data. If it does become necessary for you to need this method then you can re-enable it at a later time.

Administrative Shares

During the installation process there are default folders created on your operating system that are shared. These folders are shared to give Administrators and administrative services, such as a backup the ability to connect to certain areas of your operating system. Although a user must authenticate to the share in order to be able to access the files that are shared in that folder, the attacker will be presented with a challenge response authentication window, allowing an attacker the ability to try usernames and passwords. There are three default shares added, they are C$ (the c: drive), Admin$ (%systemroot%), and IPC$ (inter process connection). You may safely disable the C$ share and the Admin$ share by adding a registry key. You will need to add a DWORD value of AutoShareWks[v] with a value of 0 (zero) to MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters After adding the value you will need to reboot the machine. In order to verify that the shares are removed you will need to navigate to the Control Panel > Administrative Tools> Computer Management. Choose “Shares” and in the right-pane. You should now only see the IPC$ share. You cannot delete the IPC$ share because this is a share that the operating system uses to talk to itself.

Internet Explorer

The settings in this section will have to be introduced to each user profile individually.

Internet Properties

General Tab

a. Change the “Days to keep pages in History” to 0.
b. Navigate to Temporary Internet Files>Settings>”Check for newer versions of stored pages”. Change the setting to “Every time you start Internet Explorer”.
c. Navigate to “Temporary Internet Files>Settings>View Objects” and Double-Click each object and make sure that they are one's that you authorized otherwise delete

Security Tab

Make sure that each of the zones is at the “Default” level. This gives the best level of protection while maintaining functionality. As you browse websites you will be prompted to change the settings, although this may becoming annoying at times, the pop-ups will be giving you information about the data that is being process to the internet. As you browse you may want to periodically check these settings to make sure that they remain intact, later in the Group Policy snap-in, under “Administrative Templates”, you will be able to restrict the settings from begin changed.

Privacy Tab

Either choose “Medium” or navigate to “Advanced” and check “Override automatic cookie handling” and also choose to “Prompt“ so that you may have an opportunity to decide which sites you will accept cookies from. Cookies save information about your internet session. If you accept a cookie, you should remove it as soon as your session is completed.

Content Tab

a. Navigate to “Content Advisor”. If you have children you may want to enable this. This option does require you to subscribe to a Ratings Bureau.
b. Navigate to “Certificates”. You may want to get a digital id to identify yourself, there are many sites that do not support this technology as of yet.
c. Navigate to “Personal Information” and then “AutoComplete”. Uncheck “Usernames and Passwords” on Forms and then click "Clear Forms" and "Clear Passwords".

Programs Tab

The “Default” settings are recommended for this section.

Advanced

a. Click the “Restore Defaults” button.

b. Check the options
    - "Check for server certificate revocation"
    - "Check for signatures on downloaded programs"
    - "Do not save encrypted pages to disk"
    - "Empty Temporary Internet Files folder when browser is closed"
    - "Use TLS 1.0", and Uncheck "Use SSL 2.0"
c. Uncheck
    - “Use SSL 2.0” to force the browser to use 3DES and not accept DES encryption

MSN/Windows Messenger
The following setting will be on a per profiles basis, so they must be set for each user that is going to use this application. You should make sure to navigate to the “Tools” > “Options” >”Privacy” tab. It is recommended that you add in all of the users want to authorize to send instant message to you. This will prohibit unauthorized users from sending malicious html code or files that may contain viruses to you. Another recommended setting is to check “Always ask me for my password when checking Hotmail or opening other .NET Passport-enabled Web pages”. If you do not have this enabled then it will save your password on the local machine and will be able to send it to any site that you access without you knowing it. If others are using your machine you should enable “This is a shared computer so don’t display my tabs”.

Hibernation
It is recommended that you disable Hibernation under Power Settings in the Control Panel. In order to add another layer of defense, it would be necessary to not have the hibernation file on your machine. The hibernation file is not able to be encrypted. If left on your machine it could allow an attacker to be able to retrieve vital information it. This setting can be found in the Control Panel > Power Options > Hibernate tab. You will need to make sure that “Enable Hibernate” is unchecked. These settings will have to be made on a per profile basis.

Password Protected Screen Saver
One recommendation that can save a lot of worry is to enable a password protected screen saver that will lock the desktop upon activation. In the event that you are dragged away from your machine having the screen saver activate after a set period of time will help to prevent unauthorized access to the console. To enable the screen saver navigate to the Control Panel and then to Display. In the Display console, select the “Screen Saver” tab. Change the wait time to a time threshold that you feel appropriate. It is recommended to keep the default setting of ten minutes. Also make sure to check the box “On resume, password protect”, this will activate the locking of the desktop. These settings will also have to be made on a per profile basis.

TweakUI[vi]

TweakUI is a "PowerToy" utility that is freely available on Microsoft's website. You must make sure that you have Windows® XP SP1 and higher before you install this utility. This utility will allow you to set hard to find parameters. It also has a shortcut within it to allow you to open the Group Policy Microsoft Management Console, MMC, snap-in that will be discussed later. The settings that we will be primarily interested in setting will be related to the removal of data history.

1. Open the TweakUI Console.
2. Highlight "Explorer".
    a. Uncheck
        - "Allow Recent Documents on Start Menu"
        - "Allow Web content to be added to the desktop"
        - "Maintain document history"
        - "Maintain network history"
    b. Check
        - "Clear Document History on exit"
        - "Show Encrypt on the context menu"
3. Navigate to "Common Dialogs"
    a. Uncheck
        - "Enable AutoComplete"
        - "Remember previously-used filenames"
4. Navigates to "Taskbar and Start Menu" > "Start Menu"
    a. Uncheck
        - "File and Settings Transfer Wizard"
        - "Remote Assistance"
5. Navigate to "My Computer"
    a. Uncheck
        - "Files Stored on This Computer"
6. Navigate to "My Computer" > "AutoPlay" >"Drives"
    a. You should uncheck any and all drives. If you allow autoplay someone may but a CD or a USB drive into your computer that may have malicious code that will be executed.
7. Navigate to "My Computer" > "AutoPlay" >"Types"
    a. Uncheck
        - "Enable Autoplay for CD and DVD drives"
        - "Enable Autoplay for removable media"
8. Navigate to "My Computer" > "Control Panel"
    a. Since the settings set by TweakUI are all on a per profile basis you may want to disable some Control Panel icons for limited access users.
9. Navigate to "Logon"
    a. Uncheck "Parse autoexec.bat" if you do not have any applications that require information in this file. This file is a know place for viruses and Trojan Horses to write information, so that they are launched during the boot process.

10. Navigate to “Logon” > “Screen Saver”
    a. Change the setting from five seconds to 0 (zero). This default setting will allow a five second grace period from the time that the screen saver is activated until the password protected lockout is enabled.
11. Navigate to “Logon” > “Access Control”
    a. The default settings for each category are recommended, but can be hardened further on a discretionary basis.

Security Template

The most important tools to lock down your machine are the Group Policy / Local Security Policy, Security Templates combined with Administrative Templates, and the Registry. There are many sources from which to obtain Security Templates and Administrative Templates. The Administrative Templates are usually supplied by the manufacturer of the software in which you are going to restrict from the administrative level. For Microsoft Windows® XP Professional, two trusted sources from which to obtain templates are the National Security Agency and Microsoft. Both of these agencies have gone through out the operating system and have tested their policies to be secure, but to also allow for functionality. The NSA’s security template can be obtained along with their “Guide to Securing Windows XP” from their website. Microsoft’s templates can be found with the “Windows® XP Security Guide”. Both of these guided are accompanied by Security Templates that can be imported into the Local Security policy in order to lock down your Windows® XP machine. The more comprehensive of the two security templates is the one from the NSA. You should download the templates from the respective websites and then apply them as follows.

The NSA’s security template comes with an additional file, “sceregvl.inf”[vii]. This file adds entries to the registry that will be needed for workstation.inf “[viii] Security Template.

To apply the “sceregvl.inf “and security templates

1. Navigate to %SystemRoot%\inf.
2. Rename the current “sceregvl.inf” file to scregvl.inf.old
3. Copy the NSA’s “sceregvl.inf” file to the %SystemRoot%\inf folder
4. Open a command prompt.
5. Issue the command: regsvr32 scecli.dll.
6. Accept the operation by clicking “OK”.
7. Reboot the machine.
8. Once the machine is rebooted you will want to copy the “workstation.inf “ and the “High Security - Desktop.inf “or “High Security – Laptop.inf “ files to %SystemRoot%\security\templates.
9. Navigate to Start>Run and type the command “mmc” and click “OK”
10. Click File > “Add / Remove Snap-in”.
11. Click “Add”.

12. Choose “Security Configuration and Analysis” and “Security Templates” by double –clicking them.
13. Choose “Close” and “OK” to begin using the snap-ins.
14. Expand the “Security Templates” snap-in and the %SystemRoot%\security\templates tree.
15. Compare either the “High Security - Desktop.inf” or “High Security – Laptop.inf“ to the “workstation.inf” Security Template. If there are any features from the Microsoft templates that you feel will help add functionality to your NSA template then make the changes accordingly.
16. The “Restricted Groups” category has the “Power Users” group as a default but does not have any users added to it. If you plan to add any users to this group you should add them to the groups in the template before you apply it. It is recommended to add all groups and the appropriate users to them, especially the administrators group. This will help to restrict any outside attacker from elevating privileges to a group which they do not belong.
17. The section that was not edited by the NSA was the “System Services” section. This is a result of there being a wide discrepancies as to which “System Services” are need based on the configuration for each and every machine. I have added a recommendation table for the “System Services” which you can view in Appendix A. Apply the settings that are appropriate for your environment.
18. When you have the Security Template set appropriately to your configuration, choose “File” and “Save”. This will save your changes to the Security Template. It will not apply the changes to the machine.
19. Right-Click on the “Security Configuration and Analysis” snap-in and choose “Open Database”.
20. Type in a name for the database in the “File name” box. This will create the configuration database for you. Next click “Open”.
21. In the “Import Template” screen choose “workstation.inf” and click open.
22. To apply the template, again Right-click “Security Configuration and Analysis” and choose “Configure Computer Now”. Accept the path to the log file by clicking “OK”.
23. To verify the check the results of the configuration Right-click on “Security Configuration and Analysis” and choose “View Log”.
24. It is recommended to then again Right-click on “Security Configuration and Analysis’ and choose “Analyze Computer Now”, this will give final verification of the settings.

EFS

The best way to protect your data is to encrypt it. If an attacker is able to gain access to your machine they will not be able to access your data. They will only be able to gain access to your data if the attacker is able to crack your password or the attacker obtains the Default Recovery Agent. Because the Default Recovery agent will be able to recovery all encrypted files on the machine it is very important to keep it in a secure location. It is recommended that the Default

Recovery Agent be the default administrator account. The reason why this is the best possibility is that the account will be disabled. The attacker will not be able to brute-force this account and recovery the Default Recovery Agent.

a. First make sure that you have Windows XP Service Pack 1 installed and have already applied the "workstation.inf" security template from the NSA as described in the Security Template section. The reason for this is that the combination of the Service Pack and the Security Template has enabled AES-256 as the encryption algorithm. AES-256 is the strongest encryption available for EFS at the present.
b. In order to create Recovery Agent Certificate, you must go to the command prompt and issue the command: Cipher /R:Filename.[ix]
c. You must then open the Group Policy snap-in by navigating to Start>Run and issuing the command "gpedit.msc".
d. You will need to navigate to "Windows Settiings" > "Public Key Policies" > "Encrypting File System".
e. In the right-pane, you will need to right-click and select "Add Data Recovery Agent".
f. After adding the Data Recovery Agent certificates move the certificates from the Administrator profile to removable media and store them in a secure location.

You will now be able to safely encrypt all users "My Documents" folders.

Group Policy / Local Security Policy

If you want to use any administrative templates to secure any software you will need to copy them to the %SystemRoot%\security\ folder at this time, such as those provided with Microsoft Office. You can then add them to the Group Policy after opening "gpedit.msc". After opening the MMC snap-in, navigate to "Administrative Templates" and right-click. Choose "Add/Remove" templates, and click the "Add" button. Highlight the templates that you wish to add and click "OK" and then "Close". You will see the corresponding template.

In the Group Policy snap-in you may set some of the settings that you have already restricted such as Disabling Remote Desktop Sharing for Netmeeting, Restrict the ability for Users to change the Internet Explorer Security Zones and even remove the tabs so that they cannot see the settings to change them. You can Disallow Windows Messenger from being run, Turn off Autoplay, Turn off System Restore, Disable Offline Files, and remove the Security tab in Windows Explorer so that users cannot change the permissions on files. Be aware that the restrictions on the local security policy will affect all users and may prevent local machine administrators from accessing features to secure the machine. Proceed with caution when setting policies here.

TCP/IP Security

To see what ports are listening and what applications are holding them open you will want to issue the "netstat –aon" command. If a port is open and listening, it will respond back to an attacker with information about your machine. It a port is open then an attacker will also try to attack any weaknesses that may be known about the particular service that you are running. You will want to limit the amount of ports that are listening and will be able to further control activity to these ports through either ICF or a third party firewall. If you have not disabled NetBIOS over TCP/IP (NetBT) and unbound "File and Printer Sharing" you may want to do this now. This helps to stop your computer from responding to NetBIOS requests.

To protect your machine from Denial of Service attacks caused by ping sweeps, port enumeration, banner grabbing, smurf attacks, land attacks, half scans, and session hijacking there are a few registry entries that must be edited. The entries which are listed below can be found in Microsoft's "Treats and Countermeasures Guide: Security Settings in Windows Server 2003 and Windows XP".

Registry Entries added by "Tcpip_sec.vbs"[x]
Added under MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\[xi]

Subkey Registry Value Entry	Format	Recommended Value (Decimal)
EnableICMPRedirect	DWORD	0
SynAttackProtect	DWORD	1
EnableDeadGWDetect	DWORD	0
EnablePMTUDiscovery	DWORD	0
KeepAliveTime	DWORD	300,000
DisableIPSourceRouting	DWORD	2
TcpMaxConnectResponseRetransmissions	DWORD	2
TcpMaxDataRetransmissions	DWORD	3
PerformRouterDiscovery	DWORD	0
TCPMaxPortsExhausted	DWORD	5

Registry Entries added by Winsock.vbs[xii]
Added under HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\AFD\Parameters\

Subkey Registry Value Entry	Format	Recommended Value (Decimal)
DynamicBacklogGrowthDelta	DWORD	10
EnableDynamicBacklog	DWORD	1
MinimumDynamicBacklog	DWORD	20
MaximumDynamicBacklog	DWORD	20000

It is recommended to either add these entries to the registry by updating the %\SystemRoot%\inf\sceregvl.inf file or to use the “Tcpip_sec.vbs” script in the Microsoft Windows Security Resource kit.

To update “sceregvl.inf” [xiii]

1. Open the %systemroot%\inf\sceregvl.inf file in a text editor such as Notepad.

2. Navigate to the bottom of the [Register Registry Values] section and copy the following text into the file:

```
;============================== MSS Values ==============================
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\EnableICMPRedirect,4,%Enabl
eICMPRedirect%,0
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\SynAttackProtect,4,%SynAttac
kProtect%,3,0|%SynAttackProtect0%,1|%SynAttackProtect1%
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\EnableDeadGWDetect,4,%Ena
bleDeadGWDetect%,0
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\EnablePMTUDiscovery,4,%En
ablePMTUDiscovery%,0
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\KeepAliveTime,4,%KeepAliveTi
me%,3,150000|%KeepAliveTime0%,300000|%KeepAliveTime1%,600000|%KeepAliveTime2%,1
200000|%KeepAliveTime3%,2400000|%KeepAliveTime4%,3600000|%KeepAliveTime5%,72000
00|%KeepAliveTime6%
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\DisableIPSourceRouting,4,%Di
sableIPSourceRouting%,3,0|%DisableIPSourceRouting0%,1|%DisableIPSourceRouting1%,2|%D
isableIPSourceRouting2%
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxConnectResponseRetr
ansmissions,4,
%TcpMaxConnectResponseRetransmissions%,3,0|%TcpMaxConnectResponseRetransmissions
0%,1|%TcpMaxConnectResponseRetransmissions1%,2|%TcpMaxConnectResponseRetransmis
sions2%,3|%TcpMaxConnectResponseRetransmissions3%
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxDataRetransmissions,4
,%TcpMaxDataRetransmissions%,1
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\PerformRouterDiscovery,4,%P
erformRouterDiscovery%,0
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\TCPMaxPortsExhausted,4,%T
CPMaxPortsExhausted%,1
MACHINE\System\CurrentControlSet\Services\Netbt\Parameters\NoNameReleaseOnDemand,4,
%NoNameReleaseOnDemand%,0
MACHINE\System\CurrentControlSet\Control\FileSystem\NtfsDisable8dot3NameCreation,4,%Ntf
sDisable8dot3NameCreation%,0
MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoR
un,4,%NoDriveTypeAutoRun%,3,0|%NoDriveTypeAutoRun0%,255|%NoDriveTypeAutoRun1%
MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Security\WarningLevel,4,%WarningLe
vel%,3,50|%WarningLevel0%,60|%WarningLevel1%,70|%WarningLevel2%,80|%WarningLevel3
%,90|%WarningLevel4%
MACHINE\SYSTEM\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\ScreenSaverGracePeriod,4,%ScreenSaverGracePeriod%,1
MACHINE\System\CurrentControlSet\Services\AFD\Parameters\DynamicBacklogGrowthDelta,4,
%DynamicBacklogGrowthDelta%,1
MACHINE\System\CurrentControlSet\Services\AFD\Parameters\EnableDynamicBacklog,4,%Ena
bleDynamicBacklog%,0
```

MACHINE\System\CurrentControlSet\Services\AFD\Parameters\MinimumDynamicBacklog,4,%MinimumDynamicBacklog%,1
MACHINE\System\CurrentControlSet\Services\AFD\Parameters\MaximumDynamicBacklog,4,%MaximumDynamicBacklog%,3,10000|%MaximumDynamicBacklog0%,15000|%MaximumDynamicBacklog1%,20000|%MaximumDynamicBacklog2%,40000|%MaximumDynamicBacklog3%,80000|%MaximumDynamicBacklog4%,160000|%MaximumDynamicBacklog5%
MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\SafeDllSearchMode,4,%SafeDllSearchMode%,0

3. Navigate to the bottom of the [Strings] section and copy the following text into the file:

;============================== MSS Settings ==============================
EnableICMPRedirect = "MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes"
SynAttackProtect = "MSS: (SynAttackProtect) Syn attack protection level (protects against DoS)"
SynAttackProtect0 = "No additional protection, use default settings"
SynAttackProtect1 = "Connections time out sooner if a SYN attack is detected"
EnableDeadGWDetect = "MSS: (EnableDeadGWDetect) Allow automatic detection of dead network gateways (could lead to DoS)"
EnablePMTUDiscovery = "MSS: (EnablePMTUDiscovery) Allow automatic detection of MTU size (possible DoS by an attacker using a small MTU)"
KeepAliveTime = "MSS: How often keep-alive packets are sent in milliseconds"
KeepAliveTime0 ="150000 or 2.5 minutes"
KeepAliveTime1 ="300000 or 5 minutes (recommended)"
KeepAliveTime2 ="600000 or 10 minutes"
KeepAliveTime3 ="1200000 or 20 minutes"
KeepAliveTime4 ="2400000 or 40 minutes"
KeepAliveTime5 ="3600000 or 1 hour"
KeepAliveTime6 ="7200000 or 2 hours (default value)"
DisableIPSourceRouting = "MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)"
DisableIPSourceRouting0 = "No additional protection, source routed packets are allowed"
DisableIPSourceRouting1 = "Medium, source routed packets ignored when IP forwarding is enabled"
DisableIPSourceRouting2 = "Highest protection, source routing is completely disabled"
TcpMaxConnectResponseRetransmissions = "MSS: (TcpMaxConnectResponseRetransmissions) SYN-ACK retransmissions when a connection request is not acknowledged"
TcpMaxConnectResponseRetransmissions0 = "No retransmission, half-open connections dropped after 3 seconds"
TcpMaxConnectResponseRetransmissions1 = "3 seconds, half-open connections dropped after 9 seconds"
TcpMaxConnectResponseRetransmissions2 = "3 & 6 seconds, half-open connections dropped after 21 seconds"
TcpMaxConnectResponseRetransmissions3 = "3, 6, & 9 seconds, half-open connections dropped after 45 seconds"
TcpMaxDataRetransmissions = "MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default)"
PerformRouterDiscovery = "MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)"
TCPMaxPortsExhausted = "MSS: (TCPMaxPortsExhausted) How many dropped connect requests to initiate SYN attack protection (5 is recommended)"

NoNameReleaseOnDemand = "MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers"
NtfsDisable8dot3NameCreation = "MSS: Enable the computer to stop generating 8.3 style filenames"
NoDriveTypeAutoRun = "MSS: Disable Autorun for all drives"
NoDriveTypeAutoRun0 = "Null, allow Autorun"
NoDriveTypeAutoRun1 = "255, disable Autorun for all drives"
WarningLevel = "MSS: Percentage threshold for the security event log at which the system will generate a warning"
WarningLevel0 = "50%"
WarningLevel1 = "60%"
WarningLevel2 = "70%"
WarningLevel3 = "80%"
WarningLevel4 = "90%"
ScreenSaverGracePeriod = "MSS: The time in seconds before the screen saver grace period expires (0 recommended)"
DynamicBacklogGrowthDelta = "MSS: (AFD DynamicBacklogGrowthDelta) Number of connections to create when additional connections are necessary for Winsock applications (10 recommended)"
EnableDynamicBacklog = "MSS: (AFD EnableDynamicBacklog) Enable dynamic backlog for Winsock applications (recommended)"
MinimumDynamicBacklog = "MSS: (AFD MinimumDynamicBacklog) Minimum number of free connections for Winsock applications (20 recommended for systems under attack, 10 otherwise)"
MaximumDynamicBacklog = "MSS: (AFD MaximumDynamicBacklog) Maximum number of 'quasi-free' connections for Winsock applications"
MaximumDynamicBacklog0 = "10000"
MaximumDynamicBacklog1 = "15000"
MaximumDynamicBacklog2 = "20000 (recommended)"
MaximumDynamicBacklog3 = "40000"
MaximumDynamicBacklog4 = "80000"
MaximumDynamicBacklog5 = "160000"
SafeDllSearchMode = "MSS: Enable Safe DLL search mode (recommended)"

4. Save the file and close the text editor.
5. Open a command prompt window and type the command “regsvr32 scecli.dll” to re – register the SCE DLL.
6. Reboot the machine.
7. Subsequent launches of the SCE will display these custom registry values.

Antivirus Software

One key component to protect your machine from malicious software, viruses, Trojan Horses, and other exploits is antivirus. It is recommended to find antivirus software that will periodically scan all of the files on your machine. It is recommended that the software be able to update itself with new virus definitions as soon as possible. The virus scan software should be able to scan the local files on all drives as well as integrate with your email software to scan attachments and the body of the email. Some antivirus software that do have the recommended features are Trend Micro’s PC-cillin, McAfee’s VirusScan, and Symantec’s Norton Antivirus.

Firewall / IDS / HIDS Hardware and Software

As the world has change to provide the availability of high speed internet connections at home. The availability of high speed cable and DSL is allowing millions of users to attaching there computers to the internet with more bandwidth then many medium sized businesses. Since machines are connected to an internet service that is on all of the time there is an increased availability for your machine to be attacked. It is now even more important for stand-alone PC and home users to apply layers of protection by the practice "Defense in Depth". In order to establish a layered effect, it is recommended to first install a hardware firewall / router in between the internet connection and your PC. There are several brands of Cable/DSL firewalls/routers, and many of them achieve the basic functionality of blocking unsolicited traffic from the outside getting in. One feature desired in this type of device that is to be able to block specified access from the inside network (LAN) out to the internet, or egress filtering. This will not only help to block children from visiting sites that they should not, but will help to allow you to be able to block your machine from being used as a zombie and attach other machines via know vulnerabilities. You specifically may want to block NetBIOS traffic from being sent to the internet.

Although it may think that you are safe since only authorized access is coming in from the outside, but what you may not realize is that as you browse the Web files can be downloaded to your machine. When you download applications from websites, if their executables are not MD5 or SHA1 hashed you may unknowingly install a Trojan Horse. If you are browsing with a Secure Socket Layer, SSL, connection you have a tunnel open with the server on the other end. If that server has a virus it may be attached to files that you are access and be installed on your machine. Although your antivirus program should catch this type of activity, it is recommended to install a firewall or host-based intrusion detection software on your machine. Some examples of software that provide both firewall and intrusion detection features are Zone Lab's Zone Alarm, Internet Security Systems' Black Ice, Kerio's WinRoute, Symantec's Norton Internet Security Suite or Personal Firewall, and Tiny Software's Tiny Personal Firewall.

Date and Time

For authentication purposes it is very important for computers to have their time correct, especially in a Kerberos domain environment. Having the time correct is also a benefit when tracking down an intruder via your logs. One way to maintain the correct time is to synchronize with a public Network Time Protocol (NTP) server. The drawback to this is that if someone were to attempt a man-in-the-middle attack against a public NTP server you machine may be given the wrong date or may be given information that will cause a Denial of Service, DoS. As long as you have set the computer to the correct time and the system battery is working you should not have a problem. To disable this feature, navigate to Control Panel>"Date and Time Properties">"Internet Time" and uncheck "Automatically synchronize with an Internet time server".

Spyware Removal Tools

It is recommended to install some sort of Spyware removal tool. Spyware is software that is installed with your applications. It is intended to send information back to the manufacturer. This information can be as simple as the version number of the application that you installed so you can be notified of updates to the product. A negative aspect of Spyware, is that it can also send hardware and other application information to the manufacturer to allow a software manufacturer to sell your information to spam abusers. It may also be used to send username and passwords. It is highly recommended to remove any and all forms of this type of software from your machine. Examples of Spyware removal software are Lavasoft's Ad-aware, Gibson Research Corporation's OptOut, and SpyCop. For more information on Spyware please see the white paper by Symantec Security Response, "The Dangers of Spyware"[xiv] by Andre' Post.

Testing Your Settings

MBSA – Microsoft Baseline Security Advisor[xv]

Download, install and run MBSA, and follow view the recommendations that it has. This utility will check to verify that you have the latest updates and that they are installed properly. It will verify that Internet Explorer is configured properly. It will also check to make sure that there are only two administrator accounts and that all of the accounts have passwords and that they will expire.

SANS/FBI Top 20[xvi]

Navigate to the SANS Institutes' Top 20 Most Critical Internet Security Vulnerabilities. Walk through the guide and verify that your machine is protected from each of the attacks that have been outlined. Use the tools outlined in the vulnerability descriptions to test the hardening of your machine.

Port Scan

A good way to test your hardware and software firewall software is to do a port scan. If you are going to perform this type of test the best way is to get another machine and plug directly into the respective device via a crossover or straight network cable. When you do scan your machine it may become unavailable to the internet, so if you are running services on it you may want to consider the interval at which the scanning software probes your machine. Some recommend port scanning software is Portqry.exe, NMAP, SuperScan.

Conclusion

The aim of this document was to help add a comprehensive learning aid to the every growing impossibility of protecting the well being of your data. The common practices outlined in this guide are to help make users aware of the typical ways in which an attacker may try to obtain their personal data an exploit them. It is through the layered practice of "Defense in Depth" that Information Assurance is hoped to be achieved.

Appendix A[xvii]

Display Name	Service Name	Process Name	Dependencies	DEFAULT	RECOMMENDED	DESCRIPTION
Alerter	Alerter	services.exe	Workstation	Manual	Disabled	Notifies selected users and computers of administrative alerts. If the service is stopped, programs that use administrative alerts will not receive them. If this service is disabled, any services that explicitly depend on it will fail to start.
Application Layer Gateway Service	ALG	alg.exe	None	Manual	Disabled	Provides support for 3rd party protocol plug-ins for Internet Connection Sharing and the Internet Connection Firewall.
Application Management	AppMgmt	svchost.exe	None	Manual	Manual	Provides software installation services such as Assign, Publish, and Remove. Used when you modify an application i.e. Add/Remove.
Automatic Updates	wuauserv	svchost.exe	None	Automatic	Disabled	Enables the download and installation of critical Windows updates. If the service is disabled, the operating system can be manually updated at the Windows Update Web site.
Background Intelligent Transfer Service	BITS	svchost.exe	Remote Procedure Call (RPC), Workstation	Manual	Disabled	Uses idle network bandwidth to transfer data.
ClipBook	ClipSrv	clipsrv.exe	Network DDE	Manual	Disabled	Enables ClipBook Viewer to store information and share it with remote computers. If the service is stopped, ClipBook Viewer will not be able to share information with remote computers. If this service is disabled, any services that explicitly depend on it will fail to start.
COM+ Event System	EventSystem	svchost.exe	Remote Procedure Call (RPC)	Manual	Manual	Supports System Event Notification Service (SENS), which provides automatic distribution of events to subscribing Component Object Model (COM) components. If the service is stopped, SENS will close and will not be able to provide logon and logoff notifications. If this service is disabled, any services that explicitly depend on it will fail to start.
COM+ System Application	COMSysApp	dllhost.exe	Remote Procedure Call (RPC)	Manual	Manual	Manages the configuration and tracking of Component Object Model (COM)+-based components. If the service is stopped, most COM+-based components will not function properly. If this service is disabled, any services that explicitly depend on it will fail to start.
Computer Browser	Browser	svchost.exe	Server, Workstation	Automatic	Disabled	Maintains an updated list of computers on the network and supplies this list to computers designated as browsers. If this service is stopped, this list will not be updated or maintained. If this service is disabled, any services

						that explicitly depend on it will fail to start. Straightforward as can be, it keeps track of your computers on the network. If you're on a LAN, set it to Automatic. For stand alone systems, Disable is the way to go.
Cryptographic Services	CryptSvc	svchost.exe	Remote Procedure Call (RPC)	Automatic	Automatic	Provides three management services: Catalog Database Service, which confirms the signatures of Windows files; Protected Root Service, which adds and removes Trusted Root Certification Authority certificates from this computer; and Key Service, which helps enroll this computer for certificates. If this service is stopped, these management services will not function properly. If this service is disabled, any services that explicitly depend on it will fail to start. Provides the annoying boxes that pop up telling you a driver you are about to install isn't digitally signed. If you disable this service you'll be flooded with uncertified driver notifications.
DHCP Client	Dhcp	svchost.exe	AFD Networking Support Environment, NetBIOS over TCP/IP, TCP/IP Protocol Driver	Automatic	Disabled	Manages network configuration by registering and updating IP addresses and DNS names.
Distributed Link Tracking Client	TrkWks	svchost.exe	Remote Procedure Call (RPC)	Automatic	Disabled	Maintains links between NTFS files within a computer or across computers in a network domain. For those that are part of a domain -and- use NTFS it has some value in keeping links across machines up to date, especially in the case of databases updated via the network.
Distributed Transaction Coordinator	MSDTC	msdtc.exe	Remote Procedure Call (RPC), Security Accounts Manager	Manual	Disabled	Coordinates transactions that span multiple resource managers, such as databases, message queues, and file systems. If this service is stopped, these transactions will not occur. If this service is disabled, any services that explicitly depend on it will fail to start. Closely related to Distributed Link Tracking Client discussed previously. Really serves no purpose for home user systems.
DNS Client	Dnscache	svchost.exe	TCP/IP Protocol Driver	Automatic	Disabled	Resolves and caches Domain Name System (DNS) names for this computer. If this service is stopped, this computer will not be able to resolve DNS names and locate Active Directory domain controllers. If this service is disabled, any services that explicitly depend on it will fail to start. As the description above states, it caches Domain Name System (DNS) names for this computer. If disabled, it simply means the system will go upstream to resolve DNS names rather than use the cache.

Error Reporting Service	ERSvc	svchost.exe	Remote Procedure Call (RPC)	Automatic	Disabled	Allows error reporting for services and applications running in non-standard environments. This is responsible for the box that pops up wanting you to report an application error or system crash to Microsoft.
Event Log	Eventlog	services.exe	None	Automatic	Automatic	Enables event log messages issued by Windows-based programs and components to be viewed in Event Viewer. This service cannot be stopped.
Fast User Switching Compatibility	FastUserSwitching Compatibility	svchost.exe	Terminal Services	Manual	Disabled	Provides management for applications that require assistance in a multiple user environment.
Fax Service	FAX	fxssvc.exe	Plug and Play, Print Spooler, Remote Procedure Call (RPC), Telephony	Not Installed	Disabled	Provides a Fax server on the local machine.
FTP Publishing Service	NA	inetinfo.exe	IIS Admin	Not Installed	Disabled	Provides a FTP server on the local machine.
Help and Support	helpsvc	svchost.exe	Remote Procedure Call (RPC)	Automatic	Disabled	Enables Help and Support Center to run on this computer. If this service is stopped, Help and Support Center will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.
Human Interface Device Access	HidServ	svchost.exe	Remote Procedure Call (RPC)	Disabled	Disabled	Enables generic input access to Human Interface Devices (HID), which activates and maintains the use of predefined hot buttons on keyboards, remote controls, and other multimedia devices. If this service is stopped, hot buttons controlled by this service will no longer function. If this service is disabled, any services that explicitly depend on it will fail to start.
IIS Admin	IISADMIN	inetinfo.exe	Remote Procedure Call (RPC), Security Accounts Manager	Not Installed	Disabled	Management MMC for FTP, SMTP, NNTP, and WWW server on the local machine.
IMAPI CD-Burning COM Service	ImapiService	imapi.exe	None	Manual	Disabled	Manages CD recording using Image Mastering Applications Programming Interface (IMAPI). If this service is stopped, this computer will be unable to record CDs. If this service is disabled, any services that explicitly depend on it will fail to start. If you have a problem with burning CD's, check Auto Update for a patch and then set this service to Automatic.
Indexing Service	cisvc	cisvc.exe	Remote Procedure Call (RPC)	Manual	Disabled	Indexes contents and properties of files on local and remote computers; provides rapid access to files through flexible querying language.
Internet Connection Firewall/Internet	SharedAccess	svchost.exe	Application Layer Gateway	Automatic	Disabled	Provides network address translation, addressing, name

Connection Sharing			Service, Network Connections, Network Location Awareness, Remote Access Connection Manager			resolution and/or intrusion prevention services for a home or small office network. Set this service to the same setting used for Application Layer Gateway Service.
IPSEC Services	PolicyAgent	lsass.exe	IPSEC driver, Remote Procedure Call (RPC), TCP/IP Protocol Driver	Automatic	Manual	Manages IP security policy and starts the ISAKMP/Oakley (IKE) and the IP security driver. Primarily a host authentication device used with data transfer and encryption operations on a domain.
Logical Disk Manager	dmserver	svchost.exe	Plug and Play, Remote Procedure Call (RPC)	Automatic	Automatic	Detects and monitors new hard disk drives and sends disk volume information to Logical Disk Manager Administrative Service for configuration. If this service is stopped, dynamic disk status and configuration information may become out of date. If this service is disabled, any services that explicitly depend on it will fail to start. Essential to managing and updating the hard drives. Works in conjunction with Disk Management plug-in in Microsoft Management Console.
Logical Disk Manager Administrative Service	dmadmin	dmadmin.exe	Logical Disk Manager, Plug and Play, Remote Procedure Call (RPC)	Manual	Manual	Configures hard disk drives and volumes. The service only runs for configuration processes and then stops. Works in concert with Logical Disk Manager, but can be set to Manual and it will be started and stopped as stated above.
Machine Debug Manager	MDM	mdm.exe	Remote Procedure Call (RPC)	Manual	Manual	Manages local and remote debugging for Visual Studio debuggers
Message Queuing	NA	mqsvc.exe	Distributed Transaction Coordinator, Message Queuing access control, NT LM Security Support Provider, Reliable Multicast Protocol driver, Remote Procedure Call (RPC), Server	Not Installed	Disabled	Microsoft Message Queuing (MSMQ) technology enables applications running at different times to communicate across heterogeneous networks and systems that may be temporarily offline. Applications send messages to queues and read messages from queues
Message Queuing Triggers	NA	mqtgsvc.exe	Message Queuing	Not Installed	Disabled	same as above
Messenger	Messenger	services.exe	NetBIOS Interface, Plug and Play, Remote Procedure Call (RPC), Workstation	Automatic	Disabled	Transmits net send and Alerter service messages between clients and servers. This service is not related to Windows Messenger. If this service is stopped, Alerter messages will not be transmitted. If this service is disabled, any services that explicitly depend on it will fail to start.

MS Software Shadow Copy Provider	SwPrv	dllhost.exe	Remote Procedure Call (RPC)	Manual	Disabled	Manages software-based volume shadow copies taken by the Volume Shadow Copy service. If this service is stopped, software-based volume shadow copies cannot be managed. If this service is disabled, any services that explicitly depend on it will fail to start. Related to using the Microsoft Backup Utility.
Net Login	Netlogon	lsass.exe	Workstation	Automatic	Disabled	Supports pass-through authentication of account logon events for computers in a domain. Domain Authentication, used when you log into the Domain. No domain? No Net Logon needed in spite of the way the name sounds.
NetMeeting Remote Desktop Sharing	mnmsrvc	mnmsrvc.exe	None	Manual	Disabled	Enables an authorized user to access this computer remotely by using NetMeeting over a corporate intranet. If this service is stopped, remote desktop sharing will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.
Network Connections	Netman	svchost.exe	Remote Procedure Call (RPC)	Manual	Manual	Manages objects in the Network and Dial-Up Connections folder, in which you can view both local area network and remote connections.
Network DDE	NetDDE	netdde.exe	Network DDE DSDM	Manual	Disabled	Provides network transport and security for Dynamic Data Exchange (DDE) for programs running on the same computer or on different computers. If this service is stopped, DDE transport and security will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.
Network DDE DSDM	NetDDE dsdm	netdde.exe	AFD Networking Support Enviroment, TCP/IP Protocol Driver	Manual	Disabled	Manages Dynamic Data Exchange (DDE) network shares. If this service is stopped, DDE network shares will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.
Network Location Awareness (NLA)	Nla	svchost.exe	None	Manual	Disabled	Collects and stores network configuration and location information, and notifies applications when this information changes. A part of the Internet Connection Sharing (ICS) component.
NT LM Security Support Provider	NtLmSsp	lsass.exe	None	Manual	Disabled	Provides security to remote procedure call (RPC) programs that use transports other than named pipes. Provides support for Telnet and Message Queuing.
Performance Logs and Alerts	SysmonLog	smlogsvc.exe	None	Manual	Disabled	Collects performance data from local or remote computers based on preconfigured schedule parameters, then writes the data to a log or triggers an alert. If this service is stopped, performance information will not be collected. If this service is disabled, any services that explicitly depend on it will fail to start. Another way to

						monitor system performance. If the box and network stats interest you, set this to Manual. If ignorance is bliss, Disabled is the way to go.
Plug and Play	PlugPlay	services.exe	None	Automatic	Automatic	Enables a computer to recognize and adapt to hardware changes with little or no user input. Stopping or disabling this service will result in system instability.
Portable Media Serial Number	WmdmPmSp	svchost.exe	None	Automatic	Disabled	Retrieves the serial number of any portable music player connected to your computer
Print Spooler	Spooler	spoolsv.exe	Remote Procedure Call (RPC)	Automatic	Disabled	Loads files to memory for later printing.
Protected Storage	ProtectedStorage	lsass.exe	Remote Procedure Call (RPC)	Automatic	Automatic	Provides protected storage for sensitive data, such as private keys, to prevent access by unauthorized services, processes, or users. By 'sensitive data' they mean passwords, encryption data, etc. Closely tied into other 'features' like AutoComplete
QoS RSVP	RSVP	rsvp.exe	AFD Networking Support Environment, Remote Procedure Call (RPC), TCP/IP Protocol Driver	Manual	Disabled	Provides network signaling and local traffic control setup functionality for QoS-aware programs and control applets.
Remote Access Auto Connection Manager	RasAuto	svchost.exe	Remote Access Connection Manager, Telephony	Manual	Disabled	Creates a connection to a remote network whenever a program references a remote DNS or NetBIOS name or address.
Remote Access Connection Manager	RasMan	svchost.exe	Remote Procedure Call (RPC)	Manual	Disabled	Creates a network connection.
Remote Desktop Help Session Manager	RDSessMgr	sessmgr.exe	Remote Procedure Call (RPC)	Manual	Disabled	Manages and controls Remote Assistance. If this service is stopped, Remote Assistance will be unavailable. Before stopping this service, see the Dependencies tab of the Properties dialog box.
Remote Procedure Call (RPC)	RpcSs	svchost.exe	None (but everything depends on it)	Automatic	Automatic	Everything depends on this. If you disable your machine won't boot.
Remote Procedure Call (RPC) Locator	RpcLocator	locator.exe	Workstation	Manual	Disabled	Manages the RPC service database.
Remote Registry Service	RemoteRegistry	svchost.exe	None	Automatic	Disabled	Allows remote users to access your registry.
Removable Storage	NtmsSvc	svchost.exe	Remote Procedure Call (RPC)	Manual	Disabled	Used for managing removable media. Used for things like Zip Drives, Tape Drives, Graphics Pens.
RIP Listener	NA	svchost.exe	Remote Procedure Call (RPC)	Not Installed	Disabled	Routing Information Protocol
Routing and Remote Access	RemoteAccess	svchost.exe	NetBIOSGroup, Remote Procedure Call (RPC)	Manual	Disabled	Allows computers to dial into the local computer or to access it via a VPN connection.
Secondary Logon	seclogon	svchost.exe	None	Automatic	Disabled	Enables starting processes under alternate credentials. Needed for "RunAs"
Security Accounts	SamSs	lsass.exe	Remote	Automatic	Automatic	Saves profile and security

Manager			Procedure Call (RPC)			information for local users.
Server	lanmanserver	svchost.exe	None	Automatic	Disabled	Used for file and print sharing or Message Queuing.
Shell Hardware Detection	ShellHWDetection	svchost.exe	Remote Procedure Call (RPC)	Automatic	Automatic	Used for autoplay of devices like memory cards, CD drives, etc. May be required for Laptop docking stations.
Simple Mail Transport Protocol (SMTP)	SMTPSVC	inetinfo.exe	Event Log, IIS Admin	Not Installed	Disabled	Provides an outbound E-Mail server on the local machine.
Simple TCP/IP Services	NA	tcpsvcs.exe	AFD Networking Support Environment	Not Installed	Disabled	Legacy networking compatibility.
Smart Card	SCardSvr	SCardSvr.exe	Plug and Play	Manual	Disabled	Manages access to smart cards read by this computer. If this service is stopped, this computer will be unable to read smart cards. If this service is disabled, any services that explicitly depend on it will fail to start.
Smart Card Helper	SCardDrv	SCardSvr.exe	None	Manual	Disabled	Enables support for legacy non-plug and play smart-card readers used by this computer. If this service is stopped, this computer will not support legacy reader. If this service is disabled, any services that explicitly depend on it will fail to start.
SNMP Service	NA	snmp.exe	Event Log	Not Installed	Disabled	Management Service to report information about your system.
SNMP Trap Service	NA	snmptrap.exe	Event Log	Not Installed	Disabled	Management Service to report information about your system.
SSDP Discovery Service	SSDPSRV	svchost.exe	None	Manual	Disabled	Used to locate UPnP devices on your network.
System Event Notification	SENS	svchost.exe	COM+ Event System	Automatic	Automatic	Tracks system events such as Windows logon, network, and power events. Notifies COM+ Event System subscribers of these events.
System Restore Service	srservice	svchost.exe	Remote Procedure Call (RPC)	Automatic	Disabled	Creates system snap shots or restore points for returning to later.
Task Scheduler	Schedule	svchost.exe	Remote Procedure Call (RPC)	Automatic	Disabled	Enables a user to configure and schedule automated tasks on this computer. If this service is stopped, these tasks will not be run at their scheduled times. If this service is disabled, any services that explicitly depend on it will fail to start. It's used in conjunction with programs that like to run on a schedule, such as virus scanners, backups, defrag utilities, etc. If you can remember every task that needs to be done without help, disable this service.
TCP/IP NetBIOS Helper Service	LmHosts	svchost.exe	AFD Networking Support Environment, NetBIOS over TCP/IP	Automatic	Disabled	Enables support for NetBIOS over TCP/IP (NetBT) service and NetBIOS name resolution.
TCP/IP Printer Server	LPDSVC	tcpsvcs.exe	Print Spooler, TCP/IP Protocol Driver	Not Installed	Disabled	Provides legacy support for UNIX printing.

Telephony	TapiSrv	svchost.exe	Plug and Play, Remote Procedure Call (RPC)	Manual	Disabled	Provides Telephony API (TAPI) support for programs that control telephony devices and IP based voice connections on the local computer and, through the LAN, on servers that are also running the service. If you have a modem you will need to enable this.
Telnet	TlntSvr	tlntsvr.exe	NT LM Security Support Provider, Remote Procedure Call (RPC), TCP/IP Protocol Driver	Manual	Disabled	Enables a remote user to log on to this computer and run programs, and supports various TCP/IP Telnet clients, including UNIX-based and Windows-based computers. If this service is stopped, remote user access to programs might be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.
Terminal Services	TermService	svchost.exe	Remote Procedure Call (RPC)	Manual	Disabled	Allows multiple users to be connected interactively to a machine as well as the display of desktops and applications to remote computers. The underpinning of Remote Desktop (including RD for Administrators), Fast User Switching, Remote Assistance, and Terminal Server.
Themes	Themes	svchost.exe	None	Automatic	Disabled	Provides user experience theme management. If you like the themes in XP, this makes them available. Setting this to Automatic allows all users to access themes if they wish
Uninterruptible Power Supply	UPS	ups.exe	None	Manual	Disabled	Manages an uninterruptible power supply (UPS) connected to the computer.
Universal Plug and Play Device Host	UPNPhost	svchost.exe	SSDP Discovery Service	Manual	Disabled	Provides support to host Universal Plug and Play devices.
Upload Manager	uploadmgr	svchost.exe	Remote Procedure Call (RPC)	Automatic	Disabled	Manages synchronous and asynchronous file transfers between clients and servers on the network. If this service is stopped, synchronous and asynchronous file transfers between clients and servers on the network will not occur. If this service is disabled, any services that explicitly depend on it will fail to start.
Volume Shadow Copy	VSS	vssvc.exe	Remote Procedure Call (RPC)	Manual	Disabled	Manages and implements Volume Shadow Copies used for backup and other purposes. If this service is stopped, shadow copies will be unavailable for backup and the backup may fail. If this service is disabled, any services that explicitly depend on it will fail to start. Related to using the Microsoft Backup Utility. If you use it, you might want to set this to Manual, but otherwise --- Should have the same setting as MS Software Shadow Copy Provider

WebClient	WebClient	svchost.exe	WebDav Client Redirector	Automatic	Manual	Enables Windows-based programs to create, access, and modify Internet-based files. If this service is stopped, these functions will not be available. If this service is disabled, any services that explicitly depend on it will fail to start.
Windows Audio	AudioSrv	svchost.exe	Plug and Play, Remote Procedure Call (RPC)	Automatic	Automatic	Manages audio devices for Windows-based programs. If this service is stopped, audio devices and effects will not function properly. If this service is disabled, any services that explicitly depend on it will fail to start.
Windows Image Acquisition (WIA)	stisvc	svchost.exe	Remote Procedure Call (RPC)	Manual	Disabled	Provides image acquisition services for scanners and cameras.
Windows Installer	MSIServer	msiexec.exe	Remote Procedure Call (RPC)	Manual	Manual	Installs, repairs and removes software according to instructions contained in .MSI files.
Windows Management Instrumentation	Winmgmt	svchost.exe	Event Log, Remote Procedure Call (RPC)	Automatic	Automatic	Provides a common interface and object model to access management information about operating system, devices, applications and services. If this service is stopped, most Windows-based software will not function properly. If this service is disabled, any services that explicitly depend on it will fail to start.
Windows Management Instrumentation Driver Extension	Wmi	svchost.exe	None	Manual	Manual	Provides systems management information to and from drivers.
Windows Time	W32Time	svchost.exe	None	Automatic	Disabled	Maintains date and time synchronization on all clients and servers in the network. If this service is stopped, date and time synchronization will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.
Wireless Zero Configuration	WZCSVC	svchost.exe	NDIS Usermode I/O Protocol, Remote Procedure Call (RPC)	Automatic	Disabled	Provides automatic configuration for the 802.11 adapters
WMI Performance Adapter	WmiApSrv	wmiapsrv.exe	Remote Procedure Call (RPC)	Manual	Disabled	Provides performance library information from WMI HiPerf providers.
Workstation	lanmanworkstation	svchost.exe	None (but plenty depend on it)	Automatic	Automatic	Creates and maintains client network connections to remote servers. If this service is stopped, these connections will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.
World Wide Web Publishing Service	W3SVC	inetinfo.exe	IIS Admin	Not Installed	Disabled	Provides a WWW server on the local machine.

Resources

Bickel, R., M. Cook, J. Haney, M. Kerr, CT01 T. Parker, H. Parkes, "Guide to Securing Microsoft Windows XP®", Version 1.0, National Security Agency Operational Network Evaluations Division of the Systems and Network Attack Center, October 30 2002, < http://www.nsa.gov/snac/winxp/guides/wxp-1.pdf>

Bruce Fife, "Building A Secure Windows 2000 Professional Network Installation", SANS Reading Room, 2002, <http://www.sans.org/rr/papers/66/218.pdf>

Cole, Eric, Jason Fossen, Stephen Northcutt, Hal Pomeranz, SANS Security Essentials with CISSP CBK, Version 2.1, Volumes One and Two, SANS Press, February 2003.
Cox, Phillip, and Tom Sheldon, Windows 2000 Security Handbook, McGraw-Hill Osborne Media, November 27 2000.

Defense Information Systems Agency, "Secure Configuration of Windows XP Professional Security Technical Implementation Guide", Version 1, Release 8, December 3 2002

Dillard, Kurt, "Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP", ed. Reid Bannecker, John Cobb, and Jon Tobey, Microsoft.com, 2003, <http://download.microsoft.com/download/4/d/4/4d4ddedf-b630-4b94-afbf-5610983c446f/Threats_and_Countermeasures_Guide.exe>

George, Nick, "Securing Mobile Computers with Windows XP Professional", Microsoft Corporation, October 2001, < http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/winxppro/evaluate/mblsecxp.asp>

Klinder, Bernie, "Windows XP Security Checklist", Labmice.net, December 2001<http://www.labmice.net/articles/winxpsecuritychecklist.htm>

Microsoft Corporation, "Best Practices for the Encrypting File System", July 3 2003, < http://support.microsoft.com/default.aspx?scid=kb;[LN];223316>

Microsoft Corporation, "Encrypting File System in Windows XP and Windows Server 2003", August 2002, <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/winxppro/deploy/CryptFS.asp>

Microsoft Corporation, "What's New in Security for Windows XP Professional and Windows XP Home Edition", July 2001, <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/winxppro/evaluate/xpsec.asp>

Microsoft Corporation, “Windows XP Baseline Security Checklists”, 2003, <http://www.microsoft.com/technet/security/tools/chklist/xpcl.asp>

The Microsoft Windows Team, Microsoft Windows XP Professional Resource Kit, Second Edition, Microsoft Press, June 11 2003.
Post, Andre’, “The Dangers of Spyware” Symantec Security Response, January 2002, < http://www.symantec.com/avcenter/reference/dangers.of.spyware.pdf>

Scambray, Joel, and Stuart McClure, Hacking Exposed Windows 2000, 1st Edition, McGraw-Hill Osborne Media, August 29 2001.

Smith, Ben, Brian Komar, and The Microsoft Security Team, Microsoft Windows Security Resource Kit, Microsoft Press, March 12 2003.

Quinn, Tony, and Bob Partridge, “Microsoft Windows XP Security Guide”, Microsoft.com, 2003, <http://download.microsoft.com/download/e/4/9/e49db890-f683-404d-990d-7a9842145450/Windows_XP_Security_Guide.exe>

Endnotes

[i] National Security Agency Security Recommendation Guides: Defense in Depth http://nsa1.www.conxion.com/support/guides/sd-1.pdf

[ii] Bruce Fyfe, SANS Reading Room, "Building A Secure Windows® 2000 Professional Network Installation", http://www.sans.org/rr/papers/66/218.pdf

[iii] Windows & .NET Magazine Network: JSI FAQ http://www.jsifaq.com/SUBN/tip6900/rh6929.htm

[iv] Symantec.com, How to Disable or Remove Windows Scripting Host, http://securityresponse.symantec.com/avcenter/venc/data/win.script.hosting.html

[v] Microsoft.com, HOW TO: Create and Delete Hidden or Administrative Shares on Client Computers, 314984, http://support.microsoft.com/default.aspx?scid=kb;[LN];314984

[vi] Microsoft.com, Power Toys for Windows XP, http://download.microsoft.com/download/f/c/a/fca6767b-9ed9-45a6-b352-839afb2a2679/TweakUiPowertoySetup.exe

[vii] National Security Agency, Guide to Securing Windows XP, http://www.nsa.gov/snac/winxp/guides/inf/sceregvl.inf

[viii] National Security Agency, Guide to Securing Windows XP, http://www.nsa.gov/snac/winxp/guides/inf/workstation.inf

[ix] Microsoft.com, Data Protection and Recovery in Windows XP, https://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/winxppro/support/DataProt.asp

[x] Ben Smith and Elliot Lewis, Microsoft Security Resource Kt, Microsoft Press, March 12, 2003, CD

[xi] Microsoft.com, "Threats and Countermeasures Guide: Security Settings in Windows Server 2003 and Windows XP", Chapter 10 – Additional Registry Settings, http://download.microsoft.com/download/4/d/4/4d4ddedf-b630-4b94-afbf-5610983c446f/Threats_and_Countermeasures_Guide.exe

[xii] Ben Smith and Elliot Lewis, Microsoft Security Resource Kt, Microsoft Press, March 12, 2003, CD

[xiii] Microsoft.com "Threats and Countermeasures Guide: Security Settings in Windows Server 2003 and Windows XP", Chapter 10 – Additional Registry Settings, http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/topics/hardsys/tcg/tcgch10.asp

[xiv] Andre Post, Symantec Security Response, The Dangers of Spyware, http://securityresponse.symantec.com/avcenter/reference/dangers.of.spyware.pdf

[xv] Microsoft.com, MBSA, **http://download.microsoft.com/download/8/e/e/8ee73487-4d36-4f7f-92f2-2bdc5c5385b3/mbsasetup.msi**

[xvi] The SANS Institute, The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts' Consensus, http://www.sans.org/top20/

[xvii] TheElderGeek.com, Services Guide for Windows XP, http://www.theeldergeek.com/services_guide.htm