An end-users guide to basic security practices for creating a new Windows XP desktop.

Introduction:

This guide is mostly focused on creating a decently secure installation of Windows XP Professional for an end-user. While the vast majority can be applied to Windows XP Home, and OEM Restore Disk Sets, there are a few instances where these two media will need to be setup in a different manner.

Getting the necessary resources for our secure installation:

The majority of computers that are purchased come with Windows XP pre-installed. We can use this to our advantage in gathering everything we need for our secure installation; that way we don't have to connect our computer to the internet while it is vulnerable in order to update it. In this section I'll go over how to customize your base installation of Windows in a secure fashion. I've split this section into two parts, the first uses nLite on a Windows XP CD Source; while the second part uses XPLite on an OEM Restore Disk Set. The reason for using two different tools depending on if you have a bundled restore disk vs. a pure windows installation disk has to do with compatibility. Using nLite gives a much cleaner solution in that we can modify our windows installation in the pre-installation phase and then create a bootable ISO for future use. However in the case of OEM restore disks I've found a few sets where some of the value-added software bundled doesn't work properly if windows has be edited with nLite. Fortunately we can still use XPLite for post-installation editing of the our installed windows base without sacrificing any value-added software compatibility. Additionally please be aware that while nLite is a free program, XPLite is not - its about $25.*

<u>Necessary downloads for using nLite for your custom installation:</u>

- nLite (http://nuhi.msfn.org/download.html)
- Microsoft .NET Framework 1.1 (http://nuhi.msfn.org/download.html)
- Windows XP SP2 (http://www.microsoft.com/downloads/details.aspx?FamilyId=049C9DBE-3B8E-4F30-8245-9E368D3CDB5A&displaylang=en)
- Mozilla Firefox (http://www.mozilla.org/products/firefox/)
- Mozilla Thunderbird (http://www.mozilla.org/products/thunderbird/)

At this point in time it would be helpful to make a backup of CD with Mozilla Firefox, and Mozilla Thunderbird so that you will have them ready to install once we've reformatted the drive and reinstalled Windows XP with our custom installation CD. After you've created your backup copies you can proceed to Customizing Windows XP with nLite.

<u>Necessary downloads for using XPLite for your custom installation:</u>

- XPLite (http://www.litepc.com/xplite.html)
- Windows XP SP2 (http://www.microsoft.com/downloads/details.aspx?FamilyId=049C9DBE-3B8E-4F30-8245-9E368D3CDB5A&displaylang=en)
- Mozilla Firefox (http://www.mozilla.org/products/firefox/)
- Mozilla Thunderbird (http://www.mozilla.org/products/thunderbird/)

At this point it would be beneficial to make a back up CD with Mozilla Firefox, Mozilla Thunderbird, XPLite, and Windows XP Service Pack2 so that we will have them ready to use once we've reformatted and reinstalled Windows with our OEM Restore Disk set. After you've created your backup copy you can move on the Installing Windows XP.

Before we begin, I'd like to note that these particular choices are not set in stone. If you feel that you like the added features of nLite and that your value-added software isn't a priority for you, feel free to use nLite on your OEM Disk Set. However, take note that nLite only works on the Windows XP portion of your OEM Recovery Disks, so you will have to uninstall your value-added software separately everytime you use the nLite customized CDs. If the value-added software that came with your computer is an absolute necessity, I'd recommend spending the $25 on XPLite.

Pre-Installation Processing: Customizing Windows XP with nLite

nLite does its customization of Windows XP in the pre-installation stage, and presents you with an ISO image of the changes you've made to the basic windows installation. This section will focus on using nLite to slipstream service pack 2 into our Windows XP CD, removing components of Windows XP we don't need from our Windows XP CD, Windows XP interface tweaks, and burning the ISO image to a CD.

There is a step-by-step guide with photos showing how to use nLite located here: (http://nuhi.msfn.org/guide/) In addition this section will go through each option menu and demo common triage choices.

After you've specified your Windows XP Installation source, and slipstreamed Windows XP SP2 into the program, it will allow you to remove common components from the Windows XP installation CD and setup interface tweaks. A full selection of the components I kept, and the tweaks I used for the secure system in this guide, can be found in the appendix, everything else was removed from my custom installation CD.

Explanation of some customization choices made:

The first thing you will notice in the appendix summary is that despite removing Internet Explorer and Outlook Express, I kept the Internet Explorer Core (Rendering Engine). The reason for this is all of the dependencies it has, including Windows Product Activation, Windows Media Player, Help and Support system, etc. While this might seem like a large security hole, we can rather effectively restrict what the render engine can and cannot do - without sacrificing these other programs functionality. (Securing the IE rendering engine will be covered in the Post Installation Configuration section.) Windows Media Player was kept because quite a few users like it for playing WMA files on the internet and shopping at a few digital music stores like the MSN music store, Connect, and Napster - basically its there for end-user completeness.

In the tweaks section you'll notice I've cleared the pagefile on shutdown, disabled Simple File Sharing, disabled LM Hosts, and disabled File Protection (SFC). Clearing the pagefile on your hard drive is more of a privacy issue and it keeps people with access to your hard disk from having a chance of reading what you were doing in with your computer. I've disabled simple file sharing because this forces shares to be subject to both sharing privileges and NTFS file permissions where the most restrictive precipitate are the effective permissions for a file. (I'll cover using NTFS file permissions more in Post Installation Configuration.) LM Host look-ups are disabled because of a flaw in the LM hash, which actually allows hackers to decrypt the files contents for network usernames and passwords. Another workaround for this is to just use a 15+character password since the LM hash function truncates to the first 14 characters. Finally I disabled SFC because if it is left enabled it will insist on having folders for programs that are not installed, for instance C:\Program Files\MSN Gaming Zone.

Overall most of the components I removed, and tweaks I've setup are mainly what I consider to be personal best practices. As a user you might have different tastes overall and its perfectly fine to do as you like as well. Most of the options in nLite come with short explanations to keep you informed in your decision of exactly what you want to remove.

Now we are ready to burn the ISO file to disk. This can be done with any CD burning program that supports burning image files. Once you’ve burned our custom Windows XP Installation CD, you might also want to burn or in someway back up our downloads of Mozilla Firefox and Mozilla Thunderbird if you have not already done so.

In review, what we’ve done in this section is create a custom Windows XP installation CD with only the components we want; slipstreamed service pack 2 into our Windows XP installation CD so its up-to-date; and burned the ISO so that we may install it on our system. We’ve also made a copy of Mozilla Firefox and Thunderbird so we can install them on our new system without having to connect to the internet.

Installing Windows XP:

Now we will install Windows XP. If you’ve used nLite to create a custom Windows XP installation CD, the Windows XP installation will be exactly the same as if you using your original Windows XP installation CD. The only difference is that under Advanced Networking Preferences, you might want to consider disabling LMHOST lookups. (Again to help protect from the LM Hash security vulnerability.) This won’t affect most end-user experience since LMHOST file lookups are only needed when a client machine cannot find a networked computer after exhausting other kinds of lookup attempts and is not a common practice anymore.

If you are going to be installing your OEM Restore Disks, this will proceed just as normal (even if you’ve edited them with nLite). In our example of using OEM Restore Disks with XPLite; after making a back-up CD of XPLite, Firefox, Thunderbird, and Service Pack 2; this is actually the first step of securing our system since most of our windows installation customization will occur in the post-installation period.

In review of this section, we’ve created a fresh install of Windows XP on our secure system. If you used the custom Windows XP CD we created then you base installation of Windows is ready to be customized for end-user usage. If you are planning on using XPLite, then you will want to proceed to the first section of Post-Installation Configuration: Customizing Windows XP with XPLite.

Post-Installation Configuration: Customizing Windows XP with XPLite

The first step in customizing our OEM Restore Disk Installation is to first make sure its up-to-date. If service pack 2 wasn’t part of the Restore Disk Installation, we will install it now from our back-up CD. Once Windows XP has been updated to Windows XP Service Pack 2 we can begin customization with XPLite.

XPLite is a post-installation modification tool, therefore its best to execute it on a complete system since you’ll be starting with an installed package and reducing it to the precipitate you desire. The program has a very simple three step process of registration, selection of components to remove, and removal of components/reboot. Additionally you can disable Windows File Protection (SFC) therefore keeping the system from continuously rewriting directories that are not otherwise needed; again think MSN Gaming Zone.* A full listing of the equivalent choices in XPLite to mimic what we did on our secure system with nLite can be found in the appendix.

Once again we’ve kept the Internet Explorer rendering engine, and Windows Media Player. The reason for keeping the IE rendering engine is that depending on your copy of Windows XP you will need to activate it, and product activation relies on the IE rendering engine, as well as a few other system components. While WMP is very useful for certain online music stores and playback of WMA/WMV files. Again these choices of what to keep are largely personal opinion and you are free to experiment with what you like, the ones used in the example system are a compromise between security and utility. If having the IE rendering engine bothers you, we cover locking-down the IE rendering engine later in this section.

*Once you’ve finished removing components with XPLite, you might want to visit your Program Files directory and delete any directories for programs you've removed from your Windows XP installation including: NetMeeting, FrontPage, Outlook Express, Messenger, MSN Gaming Zone, etc.

Preparing our Custom Windows XP installation for the end-user:

At this point you should have your customized base installation of Windows XP running on you system. From here on out we will be putting the polish onto our system and installing necessary programs. These tweaks will be the same irrespective of what method you used earlier to create your customized Windows XP base installation.

Locking Down the Internet Explorer rendering engine:

In its default setup the IE engine is set to be unobtrusive but insecure. The reason for this insecurity is because the majority of the IE rendering engine was designed back in the early 1990s when the market was focused more on features than over all security. Since security was not a focus implementing new features opened up a lot of security issues in the IE rendering engine. By restricting what the IE rendering engine can do we can improve its effective security for the programs that depend on it to function. In our case since we will be installing Mozilla Firefox as our primary internet browser, we only need the IE rendering engine for Windows Product Activation, Manual Windows Update, Windows Media Player browsing of MSN and affiliates, and the Help and Support features of XP. Since we have a finite set of functions that we need from the IE rendering engine, its simply a matter of disabling the features we don't need.

Lets begin, under Internet Properties, in the security tab you will see that IE's security model is divided into zones; Internet, Intranet, Trusted Sites, Restricted Sites. What we can do is define for each zone, what is an is not allowed to be processes by the rendering engine. Simultaneously since we are not going to be browsing the internet with IE we can effectively turn off the features we don't need in every zone thus helping to prevent attacks that attempt to change zones for better access privileges. The zone rules I've used for the secure system we are making can be found in the appendix.

Additionally we can restrict cookies. Not all cookies are bad, and some are actually necessary for a site to "work" properly. So how much or little you restrict cookies is up to you since it is mostly a privacy issue. In our secure system we are making I've set IE to block all cookies, except ones I specify - the High setting on the cookies slider bar. For me this is not a big issue as I will only be point the IE engine at a few sites namely Windows Update, and MSN. Remember all normal internet browsing will be accomplished using Mozilla Firefox.

Paring-Down running system services:

The system services can be found under Computer Management or by looking at Services in the Administrator Tools. System services are background processes that perform many of the underlying system functions. However not all of the ones enabled by default are necessary, and some of them can leave you open to security attacks. If you'd like to learn about what every single system service does, I'd suggest reading; Microsoft Windows XP Inside Out, Ed Bott Carl Siechert, and Craig Stinson. I've included what I feel are decently sensible settings in our secure system in the appendix.

A few in particular that deserve mention are Remote Registry, Messenger, and uPnP. Remote Registry allows one to remotely access and edit a machine's registry, it is enabled by default on Windows installations. Unless you are in a large network where physically walking to the machine is more trouble than the calories are worth there is no reason for this to be running. Granted there are no known exploits for it yet, but there is no need to have more services running than you need, because it increases your exposure, and adds to system overhead. Messenger is useful for passing Alerter system messages over an intranet/internet using NetMeeting - however its also currently most used for passing Internet Messaging Spam. Therefore turning this service off will improve the overall security of the system without sacrificing functionality since we already removed NetMeeting from our base installation. I've left uPnP active and running since some printers require it and it has been patched so that the prior security flaw no longer exists.

Disabling Simple File-Sharing, and the usage of NTFS File Permissions:

Simple file-sharing while much simpler to use takes away an extremely useful tool in controlling network access rights. What simple file-sharing does is it automatically shares folders under the guest account and shares based off of sharing permissions read, write, and full control only. Once simple file-sharing is disabled, sharing rights are defined by the most restrictive precipitate of the combined rules defined by the Sharing tab, and the NT File System permissions. An example would be Sharing C:\Network\Data, and setting up Sharing permissions as Read/Write Only. Now simultaneously unless Guest has NTFS permission to read and write to that directory, anonymous users will not be able to access that folder. However if the Users group has read access to the folder, then if the network user authenticated as a user account he would have read access only. In a sense the Sharing permissions define a maximum permission set, and then you can the NTFS permission to have fine tuned control over access. While a full explanation of how NTFS File Permissions work, all the special groups that exist, and how to define a cohesive system-wide file permissions policy is beyond the scope of this guide, if you are interested you should read; Microsoft Windows XP Inside Out, Ed Bott Carl Siechert, and Craig Stinson. (Please note the Windows XP Home does not support non-simple-filesharing.)

User Accounts:

For most purposes it would be nice to use a normal user account (aka limited account in XP) however not all software plays nicely unless it has administrator privileges. This is both a fault of Microsoft for not enforcing a strict user policy or making their software compatable with stricter NTFS file permissions and third party developers for writing multi-admin friendly code instead of multi-user friendly code. If you know that the programs you want to use play nicely with a limited user account then by all means use a limited user account. If you find that your programs work well in a user account but you need to be able to share/unshare directories on a whim then go into Computer Management and move your account to the Power User group.

If you have a program that does not play well with a User or Power User account, rather than using an Administrator account full-time, try using the Run As service and running that particular program under an Administrator accounts credentials from your User or Power User account. It works similarly to the way 'sudo' does in Unix. If that solves your programs functionality problem then you won't have to use an Administrator account for everything and you can still practice good computing security.

Automatic Updates:

There are two ways you can keep your copy of Windows Updated, one is by manually going to www.windowsupdate.com while the second is letting Windows automatically update itself in the background for you. In service pack 2 windows asks you turn on automatic updates in the security center. The reason behind this is to ensure you get updates in a timely fashion, and don't forget to update windows for 2-3 years. Keeping your system up to date is helpful because security fixes, bug fixes, and sometimes new features are pushed through windows update. It would be a shame to have someone break into your computer using a security hole that has had a patch available for it. While more advanced users might want to manually update so they have more control over that gets updated, in general for the end user getting updates is more beneficial the forgetting and not getting any updates.

Configuring the Windows Firewall:

In service pack 1 the windows firewall was seen as ineffective, however in service pack 2 there are lot of changes to the firewall in addition to just being “turned on by default”. The Windows Firewall is an application based firewall, that monitors all incoming network connections. The applications you allow to connect to the internet are called “exceptions” to the default of blocking everything. Furthermore you can define specific ports or port-ranges as well as what kinds of IP protocols you wish to control.

Most free/non-free third party firewalls you can download now monitor both incoming and outgoing connections as well as executable file changes. The general assumption by most is that monitoring of outbound connections will block any viruii, trojans, spyware, etc. Compound that with the fact that there are plenty of free full-featured firewalls and outside of convenience there is no reason outside of convenience not to use one of these third party firewalls instead. However its also of note that just because a firewall monitors outgoing connections doesn’t make you more secure. Instead it mainly serves as a warning flag (like with anti-virus, and anti-spyware) letting you know that something might not be right with your system. If you chose to install a third party firewall, Windows will automatically detect it through WMI, and disable the Windows Firewall. If you happen to shutdown your third party firewall, Windows will automatically restart the Windows Firewall.

In summary a Firewall gives you an added layer of security to the system by requiring some sort of “validation” for all incoming (and with some firewalls outgoing) connection attempts. Running a firewall does not however instantly make you more secure, all firewalls have to be configured by rules, either application based or port based. How define your rules defines your level of security, just clicking “yes allow connection” to everything isn’t any better than not running a firewall at all. The draw back of running a firewall is that it adds to the overall overhead and creates a performance hit to the system. In general its good practice to look at the above tweaks like user account rights, file permissions, and services as a primary means to protect your system rather than relying mainly on a firewall.

Software Installation:

Now we have finished configuring our customized Windows XP installation. At this point we can start installing our third party applications, and getting the computer ready for everyday use. This section is not meant to give an over view of each program and how to use it, but to delineate what we are installing it to do and why we chose that program.

Mozilla Firefox:* This is going to be our main web browser. One the program has been installed you can just to launch it where it will ask if you want it as the default browser - click yes. If you want to wait until later you can set the browser as default from the “Set Default Applications” applet. At the moment Firefox is a very stable browser that was designed with security in mind. This browser does not us the IE rendering engine at all, and has support for modern features like tabbed browsing, built in search bar, and skinning.

Mozilla Thunderbird:* This will be our main mail client. Again once the program has been installed you can just to launch it where it will ask if you want it as the default browser - click yes. If you want to wait until later you can set the browser as default from the “Set Default Applications” applet. Thunderbird is a mail client that integrates well with Firefox, does not use the IE rendering engine to display mail.

*You might want to chose something else for your main browser or mail client, that is perfectly fine. However in choosing a browser and email client keep in mind that ideally you would like to use an application that does not use the IE render engine for displaying HTML. While we did lock-down the engine earlier, that does not make it perfectly safe to use, and the settings we have are not convenient to the end-user for general browsing.

Antivirus/Antispyware: Usually people also recommend to employ these programs as well. However these like outgoing connection monitoring are only “secondary prevention”. They don’t keep the attack from happening, they just act as damage control once its already occurred. Real primary prevention only occurs through using good computing habits like not running every unsigned Active-X control you find, or opening every VB email attachment “just to see what it is”. In the end its personal preference if you want to use antivirus or antispyware (or both) however don’t fall into the mindset that it some how “protects” you from getting an infection. A quick mention of the drawbacks to running these is an increase in operating system overhead and a performance increase.

Review:

We have created a customized installation of Windows XP that includes only the components we need in the base installation. We then further customized the system by limiting the vulnerability of the IE rendering engine, and using application replacements for browsing and email. We established User/Power User accounts to use in place of Administration accounts, and reviewed the need to setup sensible NTFS File Permissions for both local computer security and network shares. We also reviewed how and why to activate automatic updates for Windows XP. Finally we covered employing the Windows or third party firewall, as well as antivirus and antispyware applications. In the grand scheme of things, this is not the absolute more secure system there is, but it does strike a decent balance between security and ease-of-use. Overall however, the most important aspect to maintaining a secure system isn’t what file permissions you set, or what fancy firewall you use, but the kind of computing practices you employ every time you use your computer. In the end safe computing practice like learning how to do anything on the computer takes time and a little common sense.

Epilogue:

In case anyone was wondering to complete our secure system and make it an overall useful end-user desktop system for my parents, I’ve also installed:

OpenOffice.org
The Gimp
Trillian
Power DVD
QuickTime
iTunes
Blind Write
Acrobat Reader
PGP

...and just to be sure, since I don’t have any faith in my parents computing practices: ZoneAlarm, Norton Antivirus, and Ad-Aware.

About the Author:

Name: Vincent
Age: 23 Height: 192cm Weight: 84kg
Blood Type: A+
Favorite Foods: Pasta, Kimchee, Cheese
Likes: Running, Grass, Cooking
Dislikes: Soggy Cereal

Appendix:

nLite Component Selection List:

Accessories:

Charmap	Defragmenter	NT Backup

Drivers:

Bluetooth Support	Cameras and Camcorders	Display Adapters
Ethernet (LAN)	Firewire (1394)	InfraRed
Sound Controllers	Windows Image Acquisition	Wireless Ethernet (WLAN)

Internet Utilites:

Internet Explorer Core	TCP/IP Version 6

Multimedia:

Luna Theme	MIDI Audio Support	Speech Support
Windows Media Player	Windows Media Player 6.4	

Operating System:

16bit Support	Application Compatability Patch	Disk Clean-Up	DR. Watson
Floppy Support	Framework	Help	Manual Install and Upgrade
MDAC	Printer Support	Security Center	Shell Media Handler
Task Scheduler	Web View	Windows Scripting Host	Zip Folders

Services:

COM+	CTF Loader	Distributed Link Tracking Client	Distributed Transaction Coordinator
DNS Client	Error Reporting	Event Log	IMAPI
Indexing Service	IPSEC Policy Agent	Logical Disk Manager	Management Instrumentation
Message Queuing	Network DDE	Performance Logs and Alerts	QoS RSVP
Quality of Service	Removable Storage	Secondary Logon	Service Advertising Protocol
SNMP	System Event Notification	System Monitor	System Restore
TCP/IP NetBIOS Helper	Termainal Services	Uninterruptable Power Supply	Universal Plug and Play
Volume Shadow Copy	WebClient	Windows Firewall	Windows Time
Wireless Zero Configuration			

Tweaks:

Disable SFC (File Protection)	Merge Driver CABs	Higher Compression of Drivers	Disable Start Menu Delay
Enable Administrative tools in Start Menu	Expand Control Panel	Remove Windows Catalog from Start Menu	Disable Page File
Disable Paging of Kernel and Core-OS	Disable Pre-Fetch Cache	Clear most recently opened documents list on logoff	Clear pagefile at shutdown
Ctrl+Alt+Del is required for Classic Login	Disable Administrative Shares	Disable and Remove Documents List from Start Menu	Disable Shutdown Tracker
Disable Simple File Sharing	Disable User Process Tracking	Remove Alexa Spyware	

XPLite Component Selection List:

Advanced Components:

Active Directory Services	Application Management	Background Intelligent Transfer	Distributed Link Tracking Client
Error Reporting Service	Network DDE	Secondary Logon	Webclient
Windows Management Instrumentation Driver Extension	Windows Time	COM+	COM+ Event System
Distributed Transaction Coordinator	MDAC	IAS	MSMQ
Alerter	Computer Browser	Microsoft Network Redirector	Net Logon
NT LM Security Support Provider	Remote Procedure Call Locater	Server Message Block Mini Redirector	TCP/IP NetBIOS Helper
Workstation	Remote Access Dial-Up Support	Routing and Remote Access Support	System Event Notification
System Restore	Terminal Services	Windows Installer	Windows Management Instrumentation

Communication and Messaging:

Wireless Zero Config

Internet Utilities:

IE HTML Rendering Engine	Java Script	Windows Automatic Updates

Multimedia:

Audio Decoders	Direct Show Video	Direct X	Media Player
OpenGL Graphics Libraries	Video Playback Codecs	Volume Control	Windows Media Player 6.4
Windows Media Player 9+	Windows Media Player Skins		

Operating System Options:

Clear Service Pack Source Files	Clear the File Protection DLL Cache	Clear Pre-Fetch Cache	Core Fonts
Driver Cache	Extra Fonts	Help and Support Center	Program Compatibility Engine
Search Assistant	System Information	TWAIN Image Acquisition Drivers	User Avatars

Server Components:

Indexing Services	Indexing Service Language Resources

System Services:

Interruptible Power Supply	Universal Plug and Play

System Tools & Utilities:

DR Watson	Security Center	Security Center Background Service
Task Scheduler	Windows Script Host	ZIP Compressed Folders

Internet Explorer Rendering Engine Settings:

-	Internet	Intranet	Trusted	Restricted
Security Level	High	Medium	Medium	High

System Services:

Automatic:

Automatic Updates	Computer Browser	Cryptographic Services	DCOM Server Process Launcher
DHCP Client	Distributed Link Tracking Client	DNS Client	Error Reporting Service
Event Log	Help and Support	HID Input Device	IPSEC Services
Logical Disk Manager	Plug and Play	Protected Storage	Remote Procedure Call
Secondary Logon	Security Accounts Manager	Security Center	Server
Shell Hardware Detection	System Event Notification	System Restore Service	Task Scheduler
TCP/IP NetBIOS Helper	Themes	WebClient	Windows Audio
Windows Firewall	Windows Management Instrumentation	Windows Time	Windows User Mode Driver Framework
Wireless Zero Configuration	Work		

Manual:

Application Layer Gateway	Application Management	ASP .NET State Service	Background Intelligent Transfer Service
COM+ Event System	COM+ System Application	Distributed Transaction Coordinator	Fast User Switching Compatibility
HTTP SSL	IMAPI CD-Burning COM Service	Indexing Service	Logical Disk Manager Administrative Service
MS Software Shadow Copy Provider	Net Logon	Network Connections	Network Location Awareness
Network Provisioning Service	NT LM Security Support Provider	Performance Logs and Alerts	Portable Media Serial Number Service
QoS RSVP	Remote Access Auto Connection Manager	Remote Access Connection Manager	Remote Desktop Help Session Manager
Remote Procedure Call Locater	Removable Storage	SSDP Discovery Service	Terminal Services
Uninterruptible Power Supply	Universal Plug and Play Device Host	Volume Shadow Copy	Windows Image Acquisition
Windows Installer	Windows Management Instrumentation Driver Extensions	WMI Performance Adapter	

Disabled:

Alerter	Routing and Remote Access	Network DDE	Network DDE DSDM