Global Information Assurance Certification Paper

Methodology for Auditing The Microsoft Windows XP Operating System
By Tony Howlett
SANS GSNA Practical Assignment Version 1.2
Presented 12/19/01

TABLE OF CONTENTS

I. Windows XP Audit Methodology

A. Windows XP Security Overview:

1. Windows XP Background

Microsoft Corporation released their new Windows XP operating system with great fanfare on October 25th, 2001. It has been in development under the code name "Whistler" for several years and is Microsoft's latest attempt to merge their business and consumer operating systems. This latest offering promises better stability, easier networking, better multi-media support and better security. It is based on the NT/W2K kernel but borrows some of the better features of Windows 98 and Windows ME such as system restore.

It also requires quite a bit more hardware than previous operating systems. The recommended minimums are a 300Mhz PC with 128MB of RAM and 1.5GB of hard drive space though previous experience should tell us the folly of trying to actually use a system with the minimum specs. It also comes with a new copy protection scheme, which requires an online registration for "activation". While this feature may be an annoyance to most users and a privacy concern to some, it may actually make system administrator's jobs somewhat easier if one of their mandates is to keep a firm in compliance with licensing requirements. There are many other new features but this paper will concentrate primarily on the security features.

2. New Security Features in Windows XP [1]

Improved security features are one of the selling points of this new operating system. Some of these are improvements of existing capabilities while others are completely new additions. It is important for the audit personnel to understand these features and how they affect the security of the system. This paper will cover the features relevant to Windows XP Professional and the corporate environment. Some of these new features will not be used in the audit criteria but are included here so that personnel are fully aware of all security related issues with the operating system.

a. Group Security Policies

Windows XP allows administrators to create group security policies and apply them to multiple users easily. These Group Policy Objects ("GPOs") can make limiting network access much simpler. These privileges are similar to the file and printer access privileges in previous versions of NT but they now apply to network privileges. It also comes with sample templates such as basic, compatible, secure and highly secure to serve as examples.

b. Controlled Remote Access

This setting allows you to limit the ways someone can access your computer remotely. For those users who do not need to access their machines remotely (which will be most users), they can be set to allow only limited "guest" level privileges. This limits the damage a potential intruder can do. This is the default

setting on the basic installation.

c. Blank Password Restrictions

To keep users from using a blank password to theirs accounts, Windows XP only allows blank password logins from the console. This keeps anyone from logging into that account over the network. If the user assigns a password then network access is possible though it is affected by the limitations set in the above policy. The guest account is not affected by this and may have a blank password, however those users would be limited to the minimal privileges of the guest account.

d. Encrypting File System (EFS)

This feature from Windows 2000 has been significantly improved especially for corporate uses. It allows users to encrypt files using the DES or Triple DES so that the plain text is not stored on their hard drives. Therefore if someone were to gain access to the hard drive or download the files via some remote exploit, they would be unable to read the files. Files must be on a NTFS partition to use EFS. It is enabled by default and uses a self-signed certificate so can be used with very little administrative intervention[2]. Those who do not want to use EFS or have other issues with it will have to disable it. It can also be used with other organization that issue certificates for a fuller PKI implementation. In Windows XP, EFS may now be used to encrypt offline files and folders. It also allows you to encrypt the off-line files database that they are cached from.

e. Improved Certificate Services

Windows XP has expanded digital certificate capabilities including the ability to manage multiple levels of a CA hierarchy and a cross-certified trust network. Users may also now be auto-enrolled via a Group Policy and Active Directory. XP also supports automatic required renewal. This allows administrators to protect the certificates so that if one were compromised, it would only be useful for a short period of time.

f. Credential Management

Windows XP has some new methods to manage user sign-on and authentication. These consist of three components: credential prompting, stored user names/passwords, and the key ring. These three elements can be used together to allow a single sign-on solution. The stored username and password feature allows credentials to multiple sites and resources to be kept in a single store to permit single sign-on. The key ring allows the user to manage the credentials that are stored for them. The single-sign on feature is implemented at the application level so additional programming work may be required to take advantage of this feature. It also automates the login process, which may not be desirable from a security standpoint. For example, an unauthorized user could gain access to a user's computer when they were logged on. They could then access any other

applications that used the single sign-on.[3]

g. Fast-user switching

This feature allows users to quickly switch their login without going through logging out and logging back in. This feature is only applicable to home users not connected to a domain so this paper will not spend a lot of time on this feature.

h. Privacy

Users of Windows XP and Internet Explorer 7.0 can now manage the cookies that their system receives at a more granular level. This conforms to the P3P standard, which requires sites to provide policy information for their cookies. You can also set the browser to only accept cookies coming from trusted sources. Note: any user of IE 7.0, not just XP users gain these benefits.

i. Internet Connection Sharing

This feature greatly simplifies sharing a single Internet connection amongst several computers, which is common with smaller remote sites or telecommuters. A handy set-up wizard eliminates the need for separate proxy software or complicated settings. However, it also opens up additional security concerns such the possibility of home users putting additional home computers on a corporate Internet connection. These machines may be subject to a lower standard of security or operated by people not affiliated with the company (kids, relatives, etc). It makes the next feature and its proper configuration all the more important.

j. Internet Connection Firewall (ICF)

This new feature is probably one of the most useful from a security standpoint. It provides what has long been missing on the Windows operating system, which is awareness of security issues on the network, namely the Internet. With the growth of inexpensive broadband, many Windows users are leaving their machines, often with static, routable IP addresses wide open to the Internet. A prime example of this threat is the recent security breach at Microsoft. Their source code was exposed to a hacker who gained entry via a remote user who didn't have proper security. While the ICF is not a replacement for corporate firewalls and other measures, it certainly adds another layer of defense and for most home users, the only line of defense. Microsoft claims it as a stateful firewall, which is more than most home firewall products provide though it doesn't offer all the features of a true stateful enterprise solution[2]. The settings are pretty limited with on/off setting and a few protocols you can allow or deny. However, it is still a huge leap forward in protection for users who aren't behind a corporate firewall.

k. Software Restriction Policies

Another nice addition is the new capability to use policies to set what kinds of

software the client computers can run. The most obvious use of this is to disable java script and other applets, which cause most of the email virus trouble. There are most restrictive settings for highly secure environments that would only permit "trusted software" to run. However, in order to implement the most restrictive policies, a company would have to have a very tight control over what software etc was running and most companies don't have that capability. This feature has the most value as a malicious web-script killer.

l. IPSec Support

Continued from Windows 2000, IPSec allows for secure IP communications. It eliminates a number of potential attacks, however it does require both ends to be using IPSec. It does tend to make implementing a corporate VPN a little easier.

m. Smart card support

Combined with the Sign Sign On (SSO) implemented in Windows XP, a smart card infrastructure can be used to provide a very high level of protection for identification and authentication. Microsoft has used several industry standard for their implementation. Due to the high cost of this solution, it is unlikely that it will be deployed widely. Because of this and the hardware requirements, smart card support will not be part of our audit procedures at this time.

n. Kerberos Version 5 Support

Microsoft has included full Kerberos 5 support in Window XP Professional. Kerberos is a robust authentication and authorization system designed at MIT. It also requires a significant investment in hardware and software so for the same reasons as above, it will not be a focus of this paper

3. Other known security issues with XP

As of the date of publication of this paper, there were few published security holes in Windows XP. This is largely due to the fact that the OS has not been available to the public until recently. It may well be that this version of the OS is more secure than its predecessors as Microsoft promises. Certainly some of the features provide tools that should make a system administrator's job easier from a security standpoint. However, until it has a significant user base, it will be hard to say if the new OS is inherently more secure.

There were only two issues that were found in searches of web security sites. The first of these is a theoretical weakness. This weakness, widely debated on the web, is the inclusion of a "raw sockets" API in the OS. Some critics claim this makes it easier to use an exploited machine for DOS attacks. With this access, an attacker would not have to download and install additional tools such as a packet capture or packet editing DLL[4]. Microsoft retorts that these utilities are necessary for some of the new security features (ICF, ICS) and for the TCP stack to properly comply with standards. They also note that this exploit requires administrator privileges on the machine to be of use. There were no known tools to that took advantage of this issue

as of publication.

The second item is not really a security issue but rather a privacy issue with security implications. Microsoft's Passport authentication system is tightly integrated with Windows XP. The user is prompted several times during installation to sign up for a Passport account, which is used for authentication on Hotmail, MSN and several other sites. This system is being promoted as a Single Sign On (SSO) solution for e-commerce and websites of all kinds. The issue is that Microsoft could extend its monopoly over operating systems to financial systems and e-commerce[5]. Also, given Microsoft's history of security issues, a SSO that was breached could reveal user's financial information as well as login and password information on multiple systems, even non-Microsoft systems. In fact, during the compilation of this study, Microsoft had to take the electronic wallet portion of the Passport system offline due to a serious security flaw that was discovered. This flaw could reveal user's financial data[6]. The European Union has also expressed concerns that Passport does not comply with their consumer privacy requirements, which are much more stringent than those in the United States.

B. Designing the audit

1. Goals of the audit

This paper is designed to present a baseline for a secure Windows XP system and a methodology for auditing systems against that baseline. The goals of this audit procedure will be as follows:

- Enumerate the proper settings and configurations to use in the operating system to maintain a secure system. To this end, systems will be scored against a scale to allow for varying levels of required security and different sites requirements.
- Detail methods to verify the above settings to make sure they are configured properly and performing as intended. The methods used should be objective and quantifiable.
- Perform a sample audit on a default installation and a secured system and record the results

2. Need for the audit methodology

Microsoft has introduced a new operating system that has a number of new security features. This operating system is sure to gain a rapid user base if for no other reason than new PCs will be shipped with it by default and many smaller organizations will not bother to reinstall an earlier version. So it can be assumed that this operating system will gain rapid market share and represent an increasingly larger percentage of the user population.

Little is known of the new operating system's security. There has been little said in the press other than Microsoft's press releases and white papers. These cannot be relied upon as an objective source due to their self-serving nature. There has been some debate in the media, but most of it has been theoretical and general in nature. As of the date of this study, there has been no detailed analysis

or independent verification of the features claimed in the Microsoft literature. There are few published reports or books on the subject of Windows XP security. In absence of critical publication, most users will take Microsoft's marketing documents as fact. Additionally, there is some indication that some users may make the erroneous assumption that a new operating system will have fewer known exploits available and therefore might be more secure. This is faulty logic on two levels. First of all, Windows XP is based on the NT/W2K kernel so will be susceptible to most of the known attacks that work on those systems. Also, as the operating system proliferates, one can be sure that specific attacks and tools will quickly emerge that take advantage of the new features of the operating system. Indeed, during this study, bugs were already being discovered that had security implications[13].

As this operating system becomes a fact of life for system administrators and information security professionals, there needs to be some base line against which individual systems can be judged. A security configuration and audit methodology would provide a tool for personnel to manage system security properly. Since each organization and their security needs are different, no single configuration can be said to be the right one for every company. Therefore a multi-tiered or spectrum approach is required to give companies options for different levels of protection.

The need for a documented XP security checklist and audit procedure is clear. Millions of users of this new operating system will be flooding the Internet and corporate offices in the months to come. System administrators may think they can avoid it if their organization hasn't approved it for corporate purchase. However, they fail to take into account the telecommuters using home PCs and business partners and vendors that will need to have access to their network. These and other issues mean that IS personnel will have to understand how Windows XP affects their network security regardless of whether or not they have any Windows XP PCs in their office.

3. State of the practice

There are no published audit procedures specific to Windows XP. In fact, there is not a large amount of information on auditing Windows 2000 even a year and half after its release. The Center of Internet Security had just released its Windows 2000 scanner and checklist before this study began[7]. While NT and Windows 2000 checklists can be used for most of the features common to XP, the fact remains that XP has some new security specific features that haven't existed in any operating systems previously. One of these, the Internet Connection Firewall is an element that formerly existed in hardware firewalls. Technicians supporting end-user systems may not even manage this function. These employees may have limited knowledge of firewall technology such as access control lists and port filters that are well known to security and wide-area network personnel. Configured incorrectly, it could cause user downtime or security breaches. For example, a technician might set the firewall to deny all, disabling automated

backup program or help desk remote control software.

A search of the major online book stores produced about 50 titles related to Windows XP. None of these mention security anywhere in their descriptions. Given that these books were probably written about 6 months ago due to publishing lead times, it is likely that they used a early beta version, which may or may not act like the final release edition. A search of major Internet search engines such as Google, Yahoo and Excite generated numerous hits however most of them were articles that dealt with the "Raw Sockets" debate mentioned earlier or talked in general terms of the new features. Microsoft has several white papers, which contain a decent amount of material, but most of it simply stated that the OS was capable of a feature but didn't talk of specific configurations, much less any way to document that these features actually worked.

C. Audit Format:

The audit will consist of examining 46 items. These items will range from simple configuration settings (disabled or enabled), a range of settings, or more abstract questions such as does the machine have anti-virus software loaded. Most of these items will be fairly objective in that determining their state usually involves just checking a certain menu item. Menu locations will be given for all settings. A detailed listing of the items with descriptions follows this section. Sample worksheets that are easier to use in an actual audit will be provided in appendix B. Each item will be allotted a point value. If the audit item is in compliance (in the desired setting or condition), then the point value is earned. At the end of the audit, all point values will be added up. They can then be compared against a scale to give the relative security of the system. This spectrum approach gives a better overall view of the system security rather than just a pass or fail. The grading scale is as follows:

Total Point Score	System Rating
0-69	Insecure System
70-79	Minimally Secure System
80-89	Moderately Secure System
90-100	Highly Secure System

This grading scale was arrived at by using the author's subjective judgment in assigning point values. The point values will probably be adjusted after these initial audits and future findings. Organizations may also move the values for base level secure or highly secure to suit their own particular needs.

This paper will concentrate on Windows XP Professional edition. The Professional edition contains some of the more complex security features. Additionally, it is more likely to be installed in the corporate environment where the security professionals who are the intended audience for this paper work. The audit process developed assumes the machine is to be used as a telecommuter workstation in a remote office although settings will be given for internal LAN use as well. Since

the server version is not available yet, more advanced uses such as web-servers, e-commerce, database, etc, will not be dealt with in this paper. A separate audit will have to be developed for Windows XP Server edition once it becomes available though this paper could certain serve as a foundation.

D. Audit Criteria

There are 7 major areas that will be surveyed in our audit methodology. Each of these areas will include multiple settings, activations and configurations. All of these evaluations will be objective determinations, that is, the setting or configuration is either present or not present. Determination of point value of each item is a subjective judgment of the author based on potential threat to the computer or organization, difficulty of a potential exploit and its availability. As the operating system this audit focuses on is very new, it is fully expected the point values and summation values will be updated and appended as more experience is gained.

For each audit item, the following things will be reviewed: Item description and significance for security, where the control settings are for that item, default setting, and an optional verification procedure to confirm that the setting is working as it should. The recommended settings and configurations for the existing W2K features draws heavily from 4 sources: The NSA's Windows 2000 Security Recommendations, The SANS Security Configuration Tool and Template Settings, The Center for Internet Security's Win2000 Benchmark and Implementation Guides and Windows NT/2000: Network Security[7,8,9,10]. Some settings or recommendations from the previous lists have been intentionally left out as they are primarily server security concerns and this audit is for a Windows XP workstation machine. Also some of these have been consolidated into a single audit item. Where the lists didn't agree, generally this audit takes an average of the two. The audit items are as follows:

1. Account Policies: Minimum Password Age[7,8,9,10]

Location:	Control Panel| Performance and Maintenance| Admin Tools| Local Security Policy| Password Policy
Default Setting:	0 Days (disabled)
Desired Setting	1 day or more 1 Point
Verification:	Attempt to change password before one day
Comments:	This keeps a user from having a password with a one minute time age and cycling through all the passwords stored so as to use the same password again.

2. Account Policies: Maximum Password Age[7,8,9,10]

Location:	Control Panel| Performance and Maintenance| Admin Tools| Local Security Policy| Password Policy
Default Setting:	42 days
Desired Setting	90 days or less 2 Points
Verification:	Attempt to keep password beyond 90 days
Comments:	Here the default setting is less than the recommended.

3. Account Policies: Minimum Password Length[7,9]

Location:	Control Panel| Performance and Maintenance| Admin Tools| Local Security Policy| Password Policy
Default Setting:	0 (disabled)
Desired Setting	7 characters or more 2 Points
Verification:	Attempt to use a 6-character password
Comments:	This provides a reasonable level of protection from brute force attacks on a hashed password. This is particularly important if the system is still set to send LM or NTV1 password hashes. Also note, 8 character passwords are actually worse than 7 characters due to the way the password is hashed in two 4-character parts.

4. Account Policies: Password Complexity[7,8,9]

Location:	Control Panel| Performance and Maintenance| Admin Tools| Local Security Policy| Password Policy
Default Setting:	Disabled
Desired Setting	Enabled 2 Points
Verification:	Attempt to use a simple password of proper length such as "password"
Comments:	With this enabled, users must use passwords with some combination of letters, numbers, upper case, lower-case or special characters. This increases the difficulty of brute force attacks by orders of magnitude.

5. Account Policies: Password History[7,8,9]

Location:	Control Panel| Performance and Maintenance| Admin Tools| Local Security Policy| Password Policy
Default Setting:	0 passwords stored (disabled)
Desired Setting	24 or more 1 Point
Verification:	Attempt to use the same password when prompted to change
Comments:	This setting determines the number of old passwords that are stored for users so that they cannot reuse them. This combined with a low setting for item 1 makes reusing passwords very hard to do.

6. Account Policies: Store Passwords Using Reversible Encryption[7,9,10]

Location:	Control Panel| Performance and Maintenance| Admin Tools| Local

Security Policy| Password Policy
Default Setting: Disabled
Desired Setting Disabled 1 Point
Verification: N/A
Comments: An improvement over previous versions, this setting is disabled by default.

7. Account Policies: Account Lockout Threshold[7]
Location: Control Panel| Performance and Maintenance| Admin Tools| Local Security Policy| Account Lockout Policy
Default Setting: 0 bad logins (disabled)
Desired Setting 4 or fewer bad logins 1 Point
Verification: Attempt to login in with bad password till locked out
Comments: Settings this lower than 4 attempts can create in influx of tech support calls from users who "fat-finger" their password.

8. Account Policies: Account Lockout Time[9]
Location: Control Panel| Performance and Maintenance| Admin Tools| Local Security Policy| Account Lockout Policy
Default Setting: N/A
Desired Setting 30 minutes or more 1 Point
Verification: Attempt to login again after lockout
Comments: Accounts can still be brute forced even with lockouts if it is a patient attacker. This makes it unviable even for an insanely patient attacker.

9. Account Policies: Reset Account Lockout Counter[9]
Location: Control Panel| Performance and Maintenance| Admin Tools| Local Security Policy| Account Lockout Policy
Default Setting: N/A
Desired Setting 30 minutes or more 1 Point
Verification: Attempt to log back in after a lockout
Comments: This setting resets the attempt counter so that two incorrect logins in the morning and two in the evening don't add up to a lockout.

10. Null Account Access and Enumeration[7,9,10]
Location: Control Panel| Performance and Maintenance| Admin Tools| Local Security Policy| Password Policy
Default Setting: "Do not allow enumeration of SAM accounts"
Desired Setting
a. "Do not allow enumeration of SAM accounts" 5 points
b. "Do not allow enumeration of SAM accounts or shares" 10 points
Verification: Attempt to enumerate accounts or shares with tools such as netcat or enum
Comments: This is one of the more important settings as so many windows

exploits use these "null" accounts to attack the system or gather information. Accordingly, they have a very high point value. Windows XP disables the sharing of SAM accounts by default, which is an improvement over previous editions, however it should be set to the more restrictive setting if possible. Note: this setting can break some print and file-sharing functionality and may not be feasible in all environments.

11. Network Services[10]

Location:	Control Panel| Performance and Maintenance| Admin Tools| Services
Default Setting:	Ports 135, 139, 445, 1025, 5000
Desired Setting	a. Only ports 135, 139, 445, 1025, 5000 7 Points
	b. Only Ports 445, 1025 (N.et bios turned off) 10 Points
Verification:	Run a port scanner such as Nmap
Comments:	A workstation computer should not be running any network services other than the ones needed to communicate to other hosts. Any additional services running open up an avenue for an attacker to exploit. Particularly dangerous services are http, ftp, and telnet. By default, there are relatively few ports open. However, a port scanner should be run, especially on existing or older machines to make sure additional software has not been installed. A higher level of security can be gained by turning off Net bios if those services aren't required (for telecommuters, etc).

12. Anti-Virus Protection

Location:	Variable
Default Setting:	None
Desired Setting	a. Anti-virus software installed 5 Points
	b. Latest virus definitions installed 2 Points
	c. Auto-update service 3 Points
Verification:	N/A
Comments:	This feature is not normally part of a system specific audit list. However, the author feels that it is an integral part of system security and to declare a system without it as secure would be erroneous. Accordingly, it has a fairly high value with the highest point value being for systems with auto-update since they will be protected the soonest after a virus definition is released.

13. Event Auditing: Account Login[7,8,9,10]

Location:	Control Panel| Performance and Maintenance| Admin Tools| Local Security Policy| Audit Policy
Default Setting:	No Auditing
Desired Setting	Audit success and failure 2 Points
Verification:	Login successfully and unsuccessfully and check event log

Comments: Logging both the failures and the successful attempts can help system personnel to detect attacks in progress or trends in account usage that may point to an account being compromised. For example, a secretarial account being used at 2AM or a user with admin rights being online at 7AM when that person doesn't arrive at work till 9AM. Note: increasing audit levels will increase disk space and processor requirements, especially on a system with high login activity.

14. Event Auditing: Account Management[7,8,9,10]

Location: Control Panel| Performance and Maintenance| Admin Tools| Local Security Policy| Audit Policy
Default Setting: No Auditing
Desired Setting Audit all activity 2 Points
Verification: Add an account and add privileges and check event log
Comments: Keeping an eye on account additions and privilege assignment is a good idea. If an attacker gains access to a low level account (guest or a regular user), they will attempt to escalate privilege. This will show up on the event log. They may also reactivate a disabled account or create a new account for future use

15. Event Auditing: Login Events[7,8,9,10]

Location: Control Panel| Performance and Maintenance| Admin Tools| Local Security Policy| Audit Policy
Default Setting: No Auditing
Desired Setting Audit event failure 2 Points
Verification: N/A
Comments: This setting will let you know if certain events are failing on login. This could have important security ramifications if a firewall is failing or a security policy is not being accepted.

16. Event Auditing: Privilege Use[7,8,9,10]

Location: Control Panel| Performance and Maintenance| Admin Tools| Local Security Policy| Audit Policy
Default Setting: No Auditing
Desired Setting Audit all activity 1 Point
Verification: Perform privileged function, check event log
Comments: Good for the same reasons as #14. Can also help with finding the culprit after 'someone' changes a setting and breaks something accidentally.

17. Event Auditing: Policy Changes[7,8,9,10]

Location: Control Panel| Performance and Maintenance| Admin Tools| Local Security Policy| Audit Policy
Default Setting: No Auditing

Desired Setting	Audit all activity 1 Point
Verification:	Perform privileged function, check event log
Comments:	Good for the same reasons as #14. A subtle change to a security policy could allow an attacker to do all sorts of things undetected. Also an unauthorized change might indicate a compromised domain server.

18. Event Auditing: System Events[7,8,9,10]

Location:	Control Panel| Performance and Maintenance| Admin Tools| Local Security Policy| Audit Policy
Default Setting:	No Auditing
Desired Setting	Audit all activity 1 Point
Verification:	Perform privileged function, check event log
Comments:	Auditing things like system reboots and so forth is good for finding anomalous events and also troubleshooting intermittent problems

19. Miscellaneous Settings: Allow Eject NTFS Media[7,9]

Location:	Control Panel| Performance and Maintenance| Admin Tools| Local Security Policy| Security Options
Default Setting:	Administrator
Desired Setting	Administrator .5 Point
Verification:	Attempt to remove NTFS media as a non-privileged user
Comments:	Mostly related to physical security, keeps users from taking disk drives, zip disks, etc. Doesn't apply to FAT32 media.

20. Miscellaneous Settings: Disconnect Idle Sessions[7,8,9]

Location:	Control Panel| Performance and Maintenance| Admin Tools| Local Security Policy| Security Options
Default Setting:	15 minutes
Desired Setting	15 minutes or less .5 Point
Verification:	Establish a session, wait 15 minutes and attempt activity
Comments:	A good idea to free up processor time and also prevent session hijacking.

21. Miscellaneous Settings: Clear Virtual Memory Page file on Shutdown[7,8,9,10]

Location:	Control Panel| Performance and Maintenance| Admin Tools| Local Security Policy| Security Options
Default Setting:	Disabled
Desired Setting	Enabled .5 Point
Verification:	N/A
Comments:	Mostly a physical security benefit, it keeps someone who is able to obtain access to the physical media from reading what was in virtual memory from the previous session. Note: This setting will seriously slow down reboot.

22. Miscellaneous Settings: Auto-run on CDROM

Location:	Control Panel| Performance and Maintenance| Admin Tools| Local Security Policy| Security Options
Default Setting:	Enabled
Desired Setting	Disabled .5 Point
Verification:	Insert a CD-Rom with an auto-run program
Comments:	This setting can protect a system from being infected by a Trojan horse on a CD-ROM. It could also be used to keep users from installing their own software (No auto-run and deny access to CDROM drive).

23. Miscellaneous Settings: Restrict floppy and CDROM to local user[9]

Location:	Control Panel| Performance and Maintenance| Admin Tools| Local Security Policy| Security Options
Default Setting:	Disabled
Desired Setting	Enabled .5 Point
Verification:	Attempt to access CDROM or floppy as a remote user
Comments:	This keeps remote users from accessing CDROM or floppy media. This is low security risk unless important data is kept on removable media (such as back-ups, data files, etc)

24. Miscellaneous Settings: Do Not Display Last User Name[7,9,10]

Location:	Control Panel| Performance and Maintenance| Admin Tools| Local Security Policy| Security Options
Default Setting:	Disabled
Desired Setting	Enabled .5 Point
Verification:	See if last user name shows when logging in
Comments:	Mostly a convenience to users who consistently logon at the same machine, displaying the last user name can give attackers user names to use in future attacks. For example, a visitor to an office could casually walk through the office, tapping keyboards, just to get the login screen to come up. With enough user names, a password guessing attack might work.

25. Miscellaneous Settings: LANMAN Authentication Level[7,8,9,10]

Location:	Control Panel| Performance and Maintenance| Admin Tools| Local Security Policy| Security Options
Default Setting:	"Send both LM and NTv1 responses"
Desired Setting	"Refuse LM responses" .5 Point "Refuse LM and NTv1 responses" 1 Point
Verification:	N/A
Comments:	This features allows backward compatibility with older LANMAN systems that use a weaker password hash. This hash is easily crackable and the first NT version has also been broken. The safest setting is to refuse both unless you require connectivity to these

machines.

26. Miscellaneous Settings: Using Warning Logon Title and Banner[7,9,10]

Location:	Control Panel| Performance and Maintenance| Admin Tools| Local Security Policy| Security Options
Default Setting:	Disabled
Desired Setting	Enabled 1 Point
Verification:	See if banner comes up when logging on.
Comments:	Having the appropriate warning statement on the login banner can significantly help with a prosecution in the event of a break-in. The message should contain a warning against unauthorized access and a statement that users may be monitored when on the system. It should also be approved by the firm's legal counsel.

27. Miscellaneous Settings: Administrator Account Renamed[7,9]

Location:	Control Panel| User Accounts
Default Setting:	Named "Administrator"
Desired Setting	Changed to anything else .5 Point
Verification:	Look for user "Administrator" in user accounts
Comments:	Changing the name of the administrator account will stop some script based attacks.

28. Miscellaneous Settings: Guest Account Renamed [7,9]

Location:	Control Panel| User Accounts
Default Setting:	Named "Guest"
Desired Setting	Changed to anything else .5 Point
Verification:	Look for user "Guest" in user accounts
Comments:	Changing the name of the guest account will stop some script based attacks. This can also be accomplished by disabling the guest account, which can be done easily in Windows XP (see #45 below). Note: this may break some programs that require the use of the guest account.

29. Miscellaneous Settings: System Shutdown on Audit Failure[7,8,9]

Location:	Control Panel| Performance and Maintenance| Admin Tools| Local Security Policy| Security Options
Default Setting:	Disabled
Desired Setting	Enabled .5 Point
Verification:	N/A
Comments:	This prevents a user from filling up the event log and therefore erasing evidence of their activity. Note: This can cause down time if insufficient space is allocated to audit logs.

30. Miscellaneous Settings: Send Unencrypted Passwords to 3rd Party SMB Host[7,8,9]

Location:	Control Panel| Performance and Maintenance| Admin Tools| Local

Security Policy| Security Options
Default Setting: Disabled
Desired Setting Disabled 1 Point
Verification: N/A
Comments: This prevents the system from sending passwords in the clear to systems not capable of encryption. Note: This may break legacy applications.

31. Miscellaneous Settings: Digitally Sign Client Communications[7,8,9]

Location: Control Panel| Performance and Maintenance| Admin Tools| Local Security Policy| Security Options
Default Setting: "When possible"
Desired Setting a. "When possible" .5 Point
b. "Always" 2 Points
Verification: N/A
Comments: This provides strong verification and non-repudiation for communications coming from the client.

32. Miscellaneous Settings: Prevent Storage of Passport Credentials

Location: Control Panel| Performance and Maintenance| Admin Tools| Local Security Policy| Security Options
Default Setting: Disabled
Desired Setting Enabled .5 Point
Verification: N/A
Comments: This prevents the writing of Passport credentials to the hard drive, which is done automatically if this isn't disabled.

33. Miscellaneous Settings: Recovery Console: Automatic Admin Login[7,8,9]

Location: Control Panel| Performance and Maintenance| Admin Tools| Local Security Policy| Security Options
Default Setting: Enabled
Desired Setting Disabled .5 Point
Verification: Attempt recovery
Comments: Mostly a physical threat, this setting prevents users from entering recovery mode and getting administrator access.

34. Miscellaneous Settings: Prevent Users from Installing Printer Drivers[7,8,9,10]

Location: Control Panel| Performance and Maintenance| Admin Tools| Local Security Policy| Security Options
Default Setting: Disabled
Desired Setting Enabled .5 Point
Verification: Attempt to install printer driver as unprivileged user
Comments: Keeps users from installing printer drivers and inadvertently or purposely installing a Trojan horse.

35. Miscellaneous Settings: Unsigned Driver Installation[7,8,9]

Location:	Control Panel| Performance and Maintenance| Admin Tools| Local Security Policy| Security Options
Default Setting:	Allow
Desired Setting	"Warn but allow" .5 Point "Do not allow" 1 Point
Verification:	Attempt installation of an unsigned driver
Comments:	Similar to #34 above, this keeps unsigned drivers which could contain harmful code from being installed or at least warns when they might be installed. Legitimate manufacturers should always digitally sign their drivers though not all do yet.

36. Miscellaneous Settings: CTRL-ALT-DEL required for logon[7,9]

Location:	Control Panel| Performance and Maintenance| Admin Tools| Local Security Policy| Security Options
Default Setting:	Disabled
Desired Setting	Enabled .5 Point
Verification:	Log-off and log back on
Comments:	This provides additional security for the logon process, mostly from remote attacks. Note: This may break some remote functionality.

37. Miscellaneous Settings: Auto-log off Users When Login Time Expires[7,8,9]

Location:	Control Panel| Performance and Maintenance| Admin Tools| Local Security Policy| Security Options
Default Setting:	Disabled
Desired Setting	Enabled .5 Point
Verification:	Remain logged on past time allotted as a time limited user
Comments:	This allows administrators to set specific login times for users. For example, a receptionist account might not be needed between the hours of 6PM and 7AM or the admin might set a 24-hour straight login limit to prevent people leaving their machines logged in overnight.

38. Miscellaneous Settings: Secure Channel: Digitally Encrypt and Sign[7,8,9]

Location:	Control Panel| Performance and Maintenance| Admin Tools| Local Security Policy| Security Options
Default Setting:	"When Possible"
Desired Setting	a. "When Possible" .5 Point b. "Require strong encryption" 2 Points
Verification:	N/A
Comments:	The strongest setting is a nice security feature but probably won't be feasible for most systems that have to talk to non-W2K/XP systems.

39. New XP Features: Internet Connection Firewall ("ICF")

Location:	Menu| Network Connections| Properties| Advanced	
Default Setting:	Disabled	
Desired Setting	a. Enabled	5 Points
	b. No services allowed through	5 Points
	c. All ICMP denied	3 Points
	d. All ICMP except echo-reply denied	1 Point
	e. Set to log all dropped packets	2 Points
Verification:	Using a packet constructor program such as sendIP, attempt to send packets to the machine. Use Nmap or similar program to see if the firewall is screening the ports and denying pings as appropriate.	
Comments:	Possibly the most useful new security feature added to XP. However, ICF could interfere with some corporate VPNs so this may mitigate the usefulness for some users. It must be enabled for each network connection defined (i.e. LAN, dialup, wireless, etc).	

40. New XP Features: Internet Connection Sharing ("ICS")

Location:	Menu| Network Connections| Properties| Advanced	
Default Setting:	Disabled; network activation enabled	
Desired Setting:	Network activation disabled	1 Point
Verification:	Attempt to activate ICS remotely	
Comments:	While this feature is disabled by default, allowing network activation is dangerous as it could allow a remote user to turn it on and set the machine up to route packets. You must first click on the ICS activation button to un-gray the network activation box.	

41. New XP Features: Remote Assistance

Location:	Main Menu| My Computer| Properties| Remote	
Default Setting:	Enabled	
Desired Setting:	Disable remote assistance	1 Point
Verification:	Attempt to connect to remote desktop	
Comments:	This feature is designed to make the jobs of system administrators easier. Basically it is PCAnywhere type functionality integrated into the operating system. This feature should be turned off if not in active use. Leaving the monopoly/integration issues aside, future exploits of this code could allow an attacker to take control of the system[11].	

42. New XP Features: Auto Update

Location:	Menu| System| Properties| Auto Update	
Default Setting:	Download updates automatically	
Desired Setting:	"Notify User before downloading"	1 point
Verification:	N/A	
Comments:	This feature is a mixed bag security wise. It makes updates and	

patches easier and doesn't require an administrator to actively download and install them. However, it should be set to notify user before download to avoid the potential of future Trojan horses based on this code.

43. New XP Features: Encryption File System ("EFS")

Location:	File| Properties| Advanced
Default Setting:	Enabled (NTFS volumes only)
Desired Setting:	Encrypt "My Documents" and any other major files 5 points
Comments:	This feature is automatically available on a basic install although it requires the use of the NTFS file system. Users upgrading from 95/98/ME will be on FAT32 volumes and will have to convert to NTFS to take advantage of this feature[12].

44. New XP Features: Software Restriction Policies

Location:	Run Menu| Type "MMC"
Default Setting:	No policy
Desired Setting:	Policy that disallows any web-based scripts 3points Policy that disallows any un-trusted apps 5 points
Comments:	This feature is mainly for administrators of large domains where they can carefully control the software used by the user base. Nonetheless, if used, it can provide a very high level of protection from mal-ware type programs.

45. New XP Features: Guest Account Restrictions

Location:	Main Menu| Control Panel| User accounts
Default Setting:	Disabled
Desired Setting:	Disabled 2 points
Comments:	Making the guest account disabled by default is a nice security addition in XP. However this setting may break some legacy applications and may need to be re-activated

46. New XP Features: Blank Password Restrictions

Location:	Control Panel| Performance and Maintenance| Admin Tools| Local Security Policy| Security Options
Default Setting:	Enabled
Desired Setting:	Enabled 2 points
Verification:	Attempt to log in with a blank password
Comments:	This setting keeps users from logging into accounts remotely using a blank password. Again, this may cause problems with some older applications.

II. Sample Audits

A. System Description:

1. Operating System: The OS to be audited is the Window XP Professional Edition Upgrade, Version 2002 5.1 (build 2600.xpclient.010817-1148). The upgrade was purchased at retail on November 8, 2001, shortly after the general release. It will be upgrading Windows Millennium Edition
2. Hardware: The OS will be installed on a HP Pavilion 877C PC with a 1 Ghz AMD Athlon Processor and 128 MB RAM. This meets or exceed the minimum requirements for Windows XP
3. Role of the audited machine:
   The machine being upgraded serves as a workstation in our small home office. The machine is used for accounting and basic productivity tasks in the author's wife's consulting business. It is on a switched Ethernet network with 5 other machines. It uses a LinkSys Wireless NIC to connect to the switch. It is connected to the Internet via a cable modem connection. It is protected from the Internet by a Bastille Linux IP chains firewall. It has a private IP address which is masked via the firewall.

B. Risk Analysis:

This machine is a secondary machine used in my wife's consulting business. Given that her company is a one-person show, her computer's holds most of the valuable documents used in the business. Loss of data on this machine would be extremely harmful to her business. Being a consulting business, there are also client lists and client confidential work stored on this machine. Exposure of this data would be embarrassing at a minimum and could bring legal action at worst. Finally, accounting data is stored on this particular machine and loss of this data could impair her firm's ability to collect and bill clients.

Since this machine is located in our residence, there is little risk from a physical standpoint. The largest risk factor is the dedicated Internet connection. While the firewall serves to protect from the most common attacks and the private IP keeps it from being directly visible from the Internet, there is the possibility that the firewall could be breached. There is also a risk associated with the wireless adapter used to connect to the LAN switch. This was utilized to facilitate providing access for this machine without running new network cable. While wireless NICs are a subject of security concern, they are not dealt with in this audit. Also, considering that the system is located in a residential section of a rural area, the exposure to this risk is considered low. So the overall value of this system is high and the exposure risk is low-medium due to the firewall protection and the low physical risk.

C. Perform the Audit

The audit will be performed twice on this machine. The first time will be audit the default installation of the operating system. The author will then make certain changes to the settings to correct any problems found in the first audit. Another audit will then be performed against the machine. Not all issues turned up in the first audit may be fixed. This is a production machine and

certain settings may detract from usability more than the security value they provide, especially given the factors noted above.

See Appendix C for the checklist with auditor notes of the first audit
See Appendix D for the checklist with auditor's notes and supporting material of the second audit

D. Post Audit System Analysis

1. Default Installation Notes

This is not intended to be a complete review of the installation of the new operating system, however some security related items are of interest after going through the installation process. The installation process itself takes about an hour. It does several things that previous versions didn't. It keeps track of potential hardware or software related compatibility issues. It also automatically checks the Microsoft website and downloads any patches that have come out since that version of the CD-ROM. This is particularly useful for system administrators who are working with old disks and used to have to go through multiple layers of updates. It also gives you the option to activate the software and register. Although there are some serious privacy issues with this feature, it can help system administrators keep control of unauthorized copies of software. However since the software takes a fingerprint of the system to know which system it is authorized on, significantly changing a system's configuration can require a call to Microsoft to get a new unlocking key. Also in setting up user accounts, it didn't automatically require the user to set up passwords, which was troubling.

2. Default Installation Audit

The audit of a default installation of XP shows that it will fail to meet our specifications for a minimally secure system, which is considered "passing" for purposes of this study. There are some major improvements over how NT or other Windows operating systems are configured by default. For example, the Null account access is partially disabled and some of the other registry settings are set at a secure setting by default. Nmap shows a minimal set of network services running (net bios, listen, loc-srv, MSds, and fics). However, it is still deficient in some very important areas such as password protection and audit controls. Also, of the new security features added in Windows XP, only two are set at their most secure setting. The rest must be enabled manually. So, appropriately, the system fails the audit on a default installation

3. Post Installation Audit

This audit was performed after some changes were made in the configuration based on the results of the initial audit and on personal preferences. The first thing that was done was to configure more stringent password and audit settings. Also new anti-virus software was loaded that had auto-update features. Enabling several of the new security features considerably helped in the scoring as well. The system made the grade for being a "Moderately

Secure System" (84.5%). There were several settings in the miscellaneous section that were not set. This was primarily for usability and functionality concern. For example, clearing the virtual memory page file would make the system much slower in reboot. Since the primary security concerns of this system were remote access, the physical security settings were judged to be not as important although those that did not affect usability too much were still applied. Testing the built-in firewall produced the desired results. Nmap was unable to find any open ports or identify the system. Using the "Enum" program, we were able to verify that null sessions were properly restricted. The output of these two programs gave us reasonable assurance that some of the major settings were working as advertised. Additional verification could be done via tools such as windump, however at the time of this study, windump would not work on XP. It is suspected that this is due to the changes that Microsoft has made to their network stacks in order to make the ICF and ICS work. Based on the use and location of this machine, the rating of 84.5 was judged satisfactory to protect the system and no further action should be required for the near future.

E. Audit Methodology Analysis

This audit was designed to create a baseline for Windows XP security and a way to grade a system against that baseline. The intent was to create an audit that used a continuum to grade the system rather than a straight pass/fail. This would allow auditors and systems personnel flexibility in their system configurations to take into account specific functions and locations. A telecommuting worker's computer should have different security requirement than an accounting machine with access to payroll records. Another goal of the system was to divide the audit into several sections. These sections were weighted such that a computer must score high on at least 4 of the 7 sections in order to pass. These sections were judged to be highly important to the system security. Based on the limited tests audits done within this study, the audit seems to accomplish this goal.

Additional work will need to be done in several areas. The point values need to be tweaked to provide a proper statistical weight. More experience with systems in different environments will provide direction on which area need to be weighted more or less. Critical review of this audit will certainly generate ample opinions on the weighting scheme.

There are many areas that need to be developed further. Several of the new security features such as Kerberos, smart card and IPsec were not explored in depth in this audit due to time or budget constraints. There needs to be some attention to wireless security in the audit. Additionally, it would not be difficult to develop a script using visual basic or some similar tool that would automatically grade the system and possibly even drop the results in to a database. This project is actually being developed by the author and may be released as freeware when it is done. Finally, as the operating system matures, new exploits and bugs will be discovered. This will lead to additions or

changing of the weights in the audit items.

F. Conclusions

Windows XP has been heralded as a major advance in PC operating systems Microsoft has added many useful security tools and options that take into account the different ways that people are using their computers. It also takes into account the proliferation of cable modems, DSL and other "always-on" access technologies and the security implications that these present.

However, all these features add complexity to an already complex product. And these features must be correctly configured, controlled and managed in order to be useful. Over-worked system administrators, often doubling as their organization's info-security staff, already have their hands full applying patches and keeping up with multiple platforms and versions of software. The question remains whether computer users and systems administrators will be able to take full advantage of these new features when they can't even keep up with current patches and proper setting. The recent spread of worms such as CodeRed and Nimda using security vulnerabilities that had months old patches available are evidence of this problem. Additionally, there is some debate whether these "features" are helpful or harmful given the current lack of security understanding in the general user community. Hopefully, this audit procedure will help provide an easy way to judge Windows XP security and take corrective action if needed.

APPENDIX A
Methodology for Auditing The Microsoft Windows XP Operating System
References

1. Microsoft Corporation. "Whats New in Security for Windows XP Professional and Windows XP Home Edition". July 2001. http://www.microsoft.com/windowsxp/pro/techinfo/planning/security/whatsnew/default.asp

2. Andress, Mandy "How will Windows XP cope with security?" InfoWorld, 5/14/01. www.itworld.com/Comp/2218/IWD010514tcwindowsxp/

3. Leo, Ross. "Single Sign-on", Information Security Management Handbook, 4th Edition, pp 5-32. Aurbach Publications, 2001.

4. Gibson, Steve. "Denial of Service with Windows XP". Gibson Research Corporation, August 2001. http://grc.com/dos/winxp.htm

5. Wilcox, Joe. "Windows XP pushes Passport". ZDNET, June 2001. http://www.zdnet.com.au/newstech/news/story/0,2000025345,20233952,00.htm

6. McWilliams, Brian. "Stealing MS Passport's Wallet". HotWired, November 2, 2001. http://www.wired.com/news/technology/0,1282,48105,00.html

7. The Center for Internet Security. "Win2000 Benchmark and Implementation Guides" November 2001. http://www.cisecurity.org/

8. National Security Agency. "Windows 2000 Security Recommendation Guides" November 2001. http://nsa2.www.conxion.com/win2k/download.htm

9. SANS Institute. "Security Configuration Tool and Template Settings". December 2000. http://www.sans.org/infosecFAQ/win/settings.htm

10. Schultz, Eugene E. "Windows NT/2000 Network Security" MacMillan Technical Publishing, 2001.

11. Farrow, Rik. "Windows XP: Security by Complexity". Network Magazine, October 5, 2001. http://www.networkmagazine.com/article/NMG20011004S0009

12. Williams, Jim. "Windows XP Security". About.com, October 2001. http://netsecurity.about.com/library/weekly/aa071601a.htm

13. Microsoft Corporation. "Microsoft Security Bulletin MS01-054 (Version 2.0)". November 1, 2001. http://www.securityfocus.com/archive/1/240009

APPENDIX B
Methodology for Auditing The Microsoft Windows XP Operating System
Sample Audit Checklist

Checklist Version: **1.0**
Date of Audit:
Audit Performed by:
System Name / Number:
IP Address (if different):
MAC Address:
System Location
System User Name:
Intended Use:

Check List Items	List#	Desired Setting	Point Value	Points Earned	Validated	Auditors Comments
Account Policies						
Minimum password age	1	1 day or more	1.00			
Maximum password age:	2	90 days or less	2.00			
Minimum password length:	3	7 characters	2.00			
Password complexity:	4	Enabled	2.00			
Password History:	5	24+	1.00			
Store passwords using reversible encryption:	6	Disabled	1.00			
Account lockout threshold:	7	4 bad attempts	1.00			
Account lockout time:	8	30+ minutes	1.00			
Reset lockout counter:	9	30+ minutes	1.00			
Null Account Access						
"No anon access to SAM accounts or shares"	10a	enabled	10.00			
"No anon access to SAM accounts"	10b	enabled	5.00			
Network Services						
No network services (except as listed)	11a	135,139,445,1025	7.00			
No network services (except as listed)	11b	445,1025	3.00			
AntiVirus Protection						
Software running?	12a	Manf. & Ver.	5.00			
Definitions updated?	12b	_____ Date:	2.00			
Auto update service?	12c	_____ Running	3.00			
Event Auditing						
Audit account login:	13	success and failure	2.00			
Audit account management:	14	audit activity	2.00			
Audit login events:	15	failure	2.00			
Audit privledge use	16	audit activity	1.00			
Audit policy changes	17	audit activity	1.00			
Audit system events	18	audit activity	2.00			
Miscellaneous Settings						
Allow eject NTFS media	19	Administrator	0.50			
Disconnect idle sessions	20	15 minutes	0.50			
Clear virtual memory pagefile on shutdown	21	enabled	0.50			

Autorun on CDROM	22	disabled	0.50
Restrict floppy and CDROM to local user	23	enabled	0.50
Do not display last logon name	24	enabled	0.50
LAN Man authentication level	25a	"Refuse LM"	0.50
LAN Man authentication level	25b	"Refuse LM & NTv1"	1.00
Using Logon warning title and banner	26	enabled	1.00
Administrator account renamed	27	changed	0.50
Guest account renamed	28	changed	0.50
Shutdown system on audit failure	29	enabled	0.50
Send unencrypted passwords to SMB hosts	30	disabled	1.00
Digitally sign client communications	31a.	"When possible"	0.50
Digitally sign client communications	31b.	"Always"	2.00
Don't allow storage of passport credentials	32	"Prevent"	0.50
Prevent users from installing printer drivers	33	Enabled	0.50
Recovery Console: Automatic admin logon	34	disabled	0.50
Unsigned driver installation	35a	"Warn but allow"	0.50
Unsigned driver installation	35b	"Do not allow"	1.00
CTRL-ALT-DEL required for login	36	enabled	0.50
Auto log-off users when login time expires	37	enabled	0.50
Secure channel digital encrypt and sign:	38a	"when possible"	0.50
Secure channel digital encrypt and sign:	38b	"require strong encrypt"	2.00
New XP Features			
Internet Connection Firewall (ICF)	39a	Enabled	5.00
Internet Connection Firewall (ICF)	39b	No servers allowed	5.00
Internet Connection Firewall (ICF)	39c	all ICMP denied	3.00
Internet Connection Firewall (ICF)	39d	all ICMP denied but echo reply	1.00
Internet Connection Firewall (ICF)	39e	Log all dropped packets	2.00
Internet Connection Sharing (ICS)	40	network activation disabled	1.00
Remote Assist	41	Disabled	1.00
AutoUpdate	42	"notify before download	2.00
Encryptions File System (EFS)	43	encrypt important directories	5.00
Software Restriction Policy	44a	Disallow all VB, Java, etc	3.00
Software Restriction Policy	44b	Disallow all untrusted apps	5.00
Guest Account Restrictions	45	enabled	2.00
Blank Password Restrictions	46	enabled	2.00

Total Points

APPENDIX C
Methodology for Auditing The Microsoft Windows XP Operating System
Default Installation Audit Checklist

System Security Audit Checklist
For Microsoft Windows XP Professional
Default Installation Audit

Checklist Version:	**1.0**
Date of Audit:	**11/24/01**
Audit Performed by:	**Tony Howlett**
System Name / Number:	**Morningstar2**
IP Address (if different):	**192.168.200.4**
MAC Address:	**BSSIP 00-04-JA-OE**
System Location	**Home Office**
System User Name:	**C. Howlett**
Intended Use:	**Workstation**

Check List Items	List#	Default Setting	Point Value	Location
Account Policies				
Minimum password age	1	0	0.00	Control Panel| Performance and Maintenance| Admin T
Maximum password age:	2	42	2.00	Control Panel| Performance and Maintenance| Admin T
Minimum password length:	3	0	0.00	Control Panel| Performance and Maintenance| Admin T
Password complexity:	4	Disabled	0.00	Control Panel| Performance and Maintenance| Admin T
Password History:	5	0	0.00	Control Panel| Performance and Maintenance| Admin T
Store passwords using reversible encryption:	6	Disabled	1.00	Control Panel| Performance and Maintenance| Admin T
Account lockout threshold:	7	0	0.00	Control Panel| Performance and Maintenance| Admin T
Account lockout time:	8	Disabled	0.00	Control Panel| Performance and Maintenance| Admin T
Reset lockout counter:	9	Disabled	0.00	Control Panel| Performance and Maintenance| Admin T
Null Account Access				
"No anon access to SAM accounts or shares"	10a	No Restrictions	0.00	Control Panel| Performance and Maintenance| Admin T
"No anon access to SAM accounts"	10b	No Restrictions	5.00	Control Panel| Performance and Maintenance| Admin T
Network Services				
No network services (except as listed)	11a	135,139,445,1025	7.00	Control Panel| Performance and Maintenance| Admin t
No network services (except as listed)	11b	445,1025	0.00	Control Panel| Performance and Maintenance| Admin t
AntiVirus Protection				
Software running?	12a	None	5.00	Variable
Definitions updated?	12b	None	0.00	Variable
Auto update service?	12c	None	0.00	Variable
Event Auditing				
Audit account login:	13	no auditing	0.00	Control Panel| Performance and Maintenance| Admin T
Audit account management:	14	no auditing	0.00	Control Panel| Performance and Maintenance| Admin T
Audit login events:	15	no auditing	0.00	Control Panel| Performance and Maintenance| Admin T
Audit privledge use	16	no auditing	0.00	Control Panel| Performance and Maintenance| Admin T
Audit policy changes	17	no auditing	0.00	Control Panel| Performance and Maintenance| Admin T
Audit system events	18	no auditing	0.00	Control Panel| Performance and Maintenance| Admin T
Miscellaneous Settings				
Allow eject NTFS media	19	Administrator	0.50	Control Panel| Performance and Maintenance| Admin T
Disconnect idle sessions	20	15 minutes	0.50	Control Panel| Performance and Maintenance| Admin T

Clear virtual memory pagefile on shutdown	21	Disabled	0.00Control Panel| Performance and Maintenance| Admin T
Autorun on CDROM	22	Enabled	0.00Control Panel| Performance and Maintenance| Admin T
Restrict floppy and CDROM to local user	23	Disabled	0.00Control Panel| Performance and Maintenance| Admin T
Do not display last logon name	24	Disabled	0.00Control Panel| Performance and Maintenance| Admin T
LAN Man authentication level	25a	Send both	0.00Control Panel| Performance and Maintenance| Admin T
LAN Man authentication level	25b	Send both	0.00Control Panel| Performance and Maintenance| Admin T
Using Logon warning title and banner	26	None	0.00Control Panel| Performance and Maintenance| Admin T
Administrator account renamed	27	Administrator	0.00Main Menu| Control Panel| User accounts
Guest account renamed	28	Guest	0.00Main Menu| Control Panel| User accounts
Shutdown system on audit failure	29	Disabled	0.00Control Panel| Performance and Maintenance| Admin T
Send unencrypted passwords to SMB hosts	30	Disabled	1.00Control Panel| Performance and Maintenance| Admin T
Digitally sign client communications	31a.	Enabled	0.50Control Panel| Performance and Maintenance| Admin T
Digitally sign client communications	31b.	Disabled	0.00Control Panel| Performance and Maintenance| Admin T
Don't allow storage of passport credentials	32	Disabled	0.00Control Panel| Performance and Maintenance| Admin T
Prevent users from installing printer drivers	33	Disabled	0.00Control Panel| Performance and Maintenance| Admin T
Recovery Console: Automatic admin logon	34	Disabled	0.50Control Panel| Performance and Maintenance| Admin T
Unsigned driver installation	35a	Allow	0.00Control Panel| Performance and Maintenance| Admin T
Unsigned driver installation	35b	Allow	0.00Control Panel| Performance and Maintenance| Admin T
CTRL-ALT-DEL required for login	36	Not defined	0.00Control Panel| Performance and Maintenance| Admin T
Auto log-off users when login time expires	37	Disabled	0.00Control Panel| Performance and Maintenance| Admin T
Secure channel digital encrypt and sign:	38a	Enabled	0.50Control Panel| Performance and Maintenance| Admin T
Secure channel digital encrypt and sign:	38b	Disabled	0.00Control Panel| Performance and Maintenance| Admin T
New XP Features			
Internet Connection Firewall (ICF)	39a	Disabled	0.00Menu| Network Connections| Properties| Advanced
Internet Connection Firewall (ICF)	39b	N/A	0.00Menu| Network Connections| Properties| Advanced
Internet Connection Firewall (ICF)	39c	N/A	0.00Menu| Network Connections| Properties| Advanced
Internet Connection Firewall (ICF)	39d	N/A	0.00Menu| Network Connections| Properties| Advanced
Internet Connection Firewall (ICF)	39e	N/A	0.00Menu| Network Connections| Properties| Advanced
Internet Connection Sharing (ICS)	40	Enabled	0.00Menu| Network Connections| Properties| Advanced
Remote Assist	41	Enabled	0.00Main Menu| My Computer| Properties| Remote
AutoUpdate	42	Download automatically	0.00Menu| System| Properties| Autoupdate
Encryptions File System (EFS)	43	no files encrypted	0.00File| Properties| Advanced
Software Restriction Policy	44a	None	0.00Added using MMC
Software Restriction Policy	44b	None	0.00Added using MMC
Guest Account Restrictions	45	Enabled	2.00Main Menu| Control Panel| User accounts
Blank Password Restrictions	46	Enabled	2.00Control Panel| Performance and Maintenance| Admin T
Total Points			**27.50**

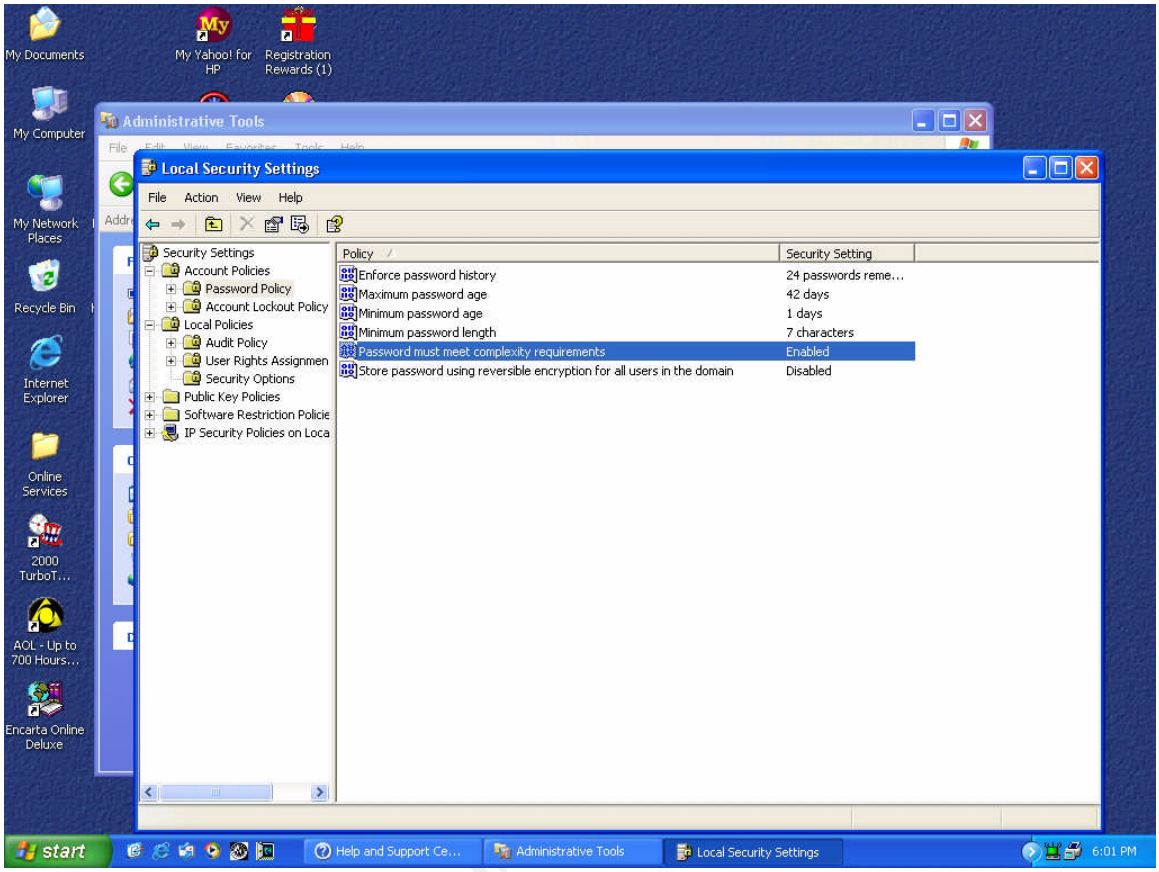
APPENDIX D
Methodology for Auditing The Microsoft Windows XP Operating System
Post Install Audit Checklist (with supporting material)

Checklist Version:	**1.0**
Date of Audit:	**11/24/01**
Audit Performed by:	**Tony Howlett**
System Name / Number:	**Morningstar2**
IP Address (if different):	**192.168.200.4**
MAC Address:	**BSSIP 00-04-JA-OE**
System Location	**Home Office**
System User Name:	**C. Howlett**
Intended Use:	**Workstation**

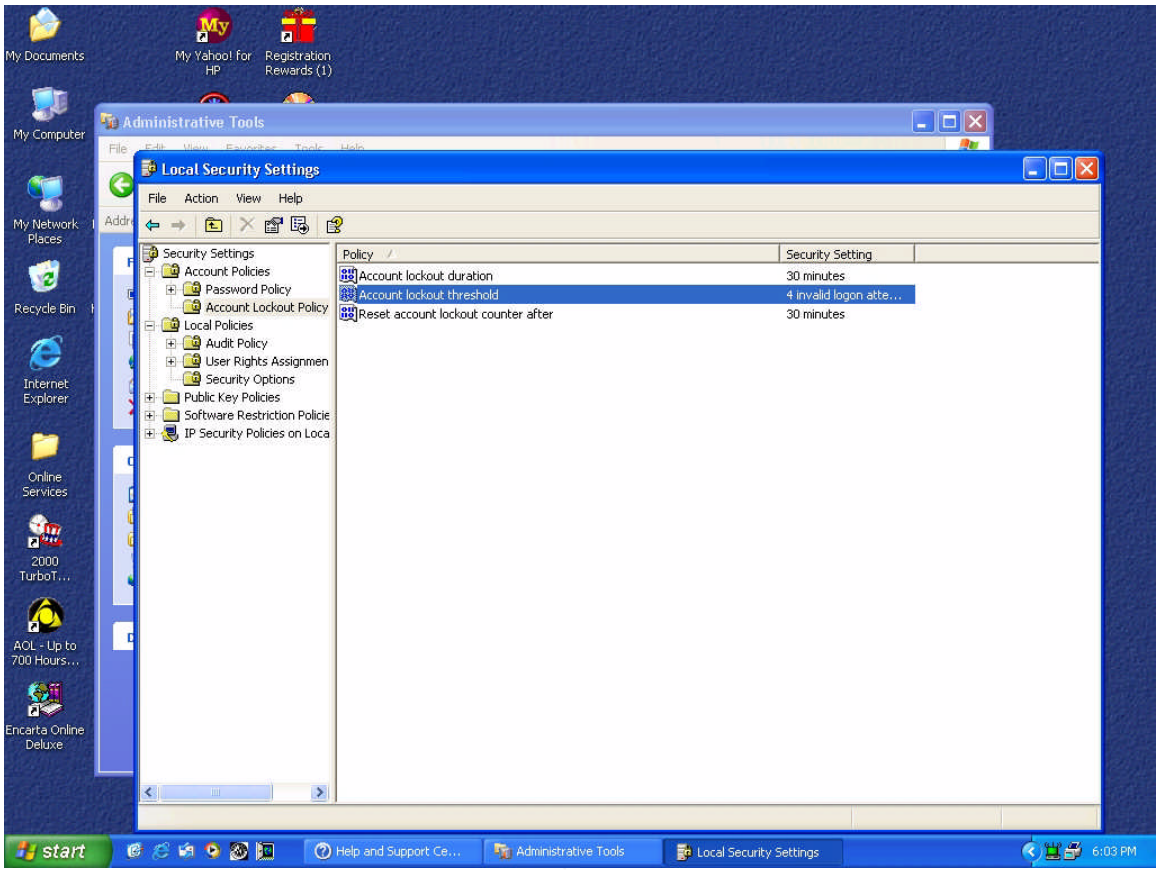
Check List Items	List#	Desired Setting	Point Value	Points Earned	Validated	Auditors Comments
Account Policies						
Minimum password age	1	1 day or more	1.00	1.00	Y	See appendix D.3 and Audit Log
Maximum password age:	2	90 days or less	2.00	2.00	N	Not enough time to validate
Minimum password length:	3	7 characters	2.00	2.00	Y	See D.3 and Audit Log D.8
Password complexity:	4	Enabled	2.00	2.00	Y	See D.3 and Audit Log D.8
Password History:	5	24+	1.00	1.00	N	Not enough time to validate
Store passwords using reversible encryption:	6	Disabled	1.00	1.00	N	Not easy to validate
Account lockout threshold:	7	4 bad attempts	1.00	1.00	Y	See D.3 and Audit Log D.8
Account lockout time:	8	30+ minutes	1.00	1.00	Y	See D.3 and Audit Log D.8
Reset lockout counter:	9	30+ minutes	1.00	1.00	Y	See D.3 and Audit Log D.8
Null Account Access						
"No anon access to SAM accounts or shares"	10a	enabled	10.00	10.00	Y	See D.8 "Enum" output
"No anon access to SAM accounts"	10b	enabled	5.00	5.00	Y	See D.8 "Enum" output
Network Services						
No network services (except as listed)	11a	135,139,445,1025	7.00	7.00	Y	See D.6.1 and D.6.2 "Nmap" ou
No network services (except as listed)	11b	445,1025	3.00	0.00	N	Needed Netbios for local office
AntiVirus Protection						
Software running?	12a	Installed	5.00	5.00	N/A	MacAfee Pro 6.0
Definitions updated?	12b	Date of update	2.00	2.00	N/A	Updated 11/30/01
Auto update service?	12c	Running	3.00	3.00	N/A	Built into 6.0
Event Auditing						
Audit account login:	13	success and failure	2.00	2.00	Y	See D.3 Audit Log
Audit account management:	14	audit activity	2.00	2.00	Y	See D.3 Audit Log
Audit login events:	15	failure	2.00	2.00	Y	See D.3 Audit Log
Audit privledge use	16	audit activity	1.00	1.00	Y	See D.3 Audit Log
Audit policy changes	17	audit activity	1.00	1.00	Y	See D.3 Audit Log
Audit system events	18	audit activity	2.00	2.00	Y	See D.3 Audit Log
Miscellaneous Settings						
Allow eject NTFS media	19	Administrator	0.50	0.50	Y	See D.4.1 & D.4.2 Security Poli
Disconnect idle sessions	20	15 minutes	0.50	0.50	Y	See D.4.1 & D.4.2 Security Poli
Clear virtual memory pagefile on shutdown	21	enabled	0.50	0.00	N	Not set for usability concerns
Autorun on CDROM	22	disabled	0.50	0.00	Y	See D.4.1 & D.4.2 Security Poli

Restrict floppy and CDROM to local user	23	enabled	0.50	0.50Y	See D.4.1 & D.4.2 Security Poli
Do not display last logon name	24	enabled	0.50	0.50Y	See D.4.1 & D.4.2 Security Poli
LAN Man authentication level	25a	"Refuse LM"	0.50	0.00N	
LAN Man authentication level	25b	"Refuse LM & NTv1"	1.00	1.00N	Not easily validated
Using Logon warning title and banner	26	enabled	1.00	1.00Y	See D.4.1 & D.4.2 Security Poli
Administrator account renamed	27	changed	0.50	0.50Y	See D.10 Users accounts
Guest account renamed	28	changed	0.50	0.50Y	See D.10 Users accounts
Shutdown system on audit failure	29	enabled	0.50	0.50Y	Production system. Unable to fi
Send unencrypted passwords to SMB hosts	30	disabled	1.00	1.00N	Not easily validated
Digitally sign client communications	31a.	"When possible"	0.50	0.50N	Not easily validated
Digitally sign client communications	31b.	"Always"	2.00	0.00N	N/A
Don't allow storage of passport credentials	32	"Prevent"	0.50	0.50N	Not easily validated
Prevent users from installing printer drivers	33	Enabled	0.50	0.50Y	See D.4.1 & D.4.2 Security Poli
Recovery Console: Automatic admin logon	34	disabled	0.50	0.50Y	See D.4.1 & D.4.2 Security Poli
Unsigned driver installation	35a	"Warn but allow"	0.50	0.50N	Not easily validated
Unsigned driver installation	35b	"Do not allow"	1.00	0.00N	
CTRL-ALT-DEL required for login	36	enabled	0.50	0.50Y	See D.4.1 & D.4.2 Security Poli
Auto log-off users when login time expires	37	enabled	0.50	0.50Y	See D.4.1 & D.4.2 Security Poli
Secure channel digital encrypt and sign:	38a	"when possible"	0.50	0.50N	Not easily validated
Secure channel digital encrypt and sign:	38b	"require strong encrypt"	2.00	0.00N	
New XP Features					
Internet Connection Firewall (ICF)	39a	Enabled	5.00	5.00Y	See D.5 Firewall Settings & D.6
Internet Connection Firewall (ICF)	39b	No servers allowed	5.00	5.00Y	See D.5 Firewall Settings & D.6
Internet Connection Firewall (ICF)	39c	all ICMP denied	3.00	0.00N	N/A
Internet Connection Firewall (ICF)	39d	all ICMP denied but echo reply	1.00	1.00Y	See D.5 Firewall Settings & D.6
Internet Connection Firewall (ICF)	39e	Log all dropped packets	2.00	2.00Y	See D.5 Firewall Settings & D.6
Internet Connection Sharing (ICS)	40	network activation disabled	1.00	1.00Y	See D.5 Firewall Settings
Remote Assist	41	Disabled	1.00	1.00Y	See D.9 Remote Assist Settings
AutoUpdate	42	"notify before download	2.00	1.00Y	See D.9.1 Autoupdate Settings
Encryptions File System (EFS)	43	encrypt important directories	5.00	0.00N	N/A
Software Restriction Policy	44a	Disallow all VB, Java, etc	3.00	0.00N	N/A
Software Restriction Policy	44b	Disallow all untrusted apps	5.00	0.00N	N/A
Guest Account Restrictions	45	enabled	2.00	2.00Y	See D.10 user accounts
Blank Password Restrictions	46	enabled	2.00	2.00Y	See D.4.1 & D.4.2 Security Poli
Total Points				**84.50**	

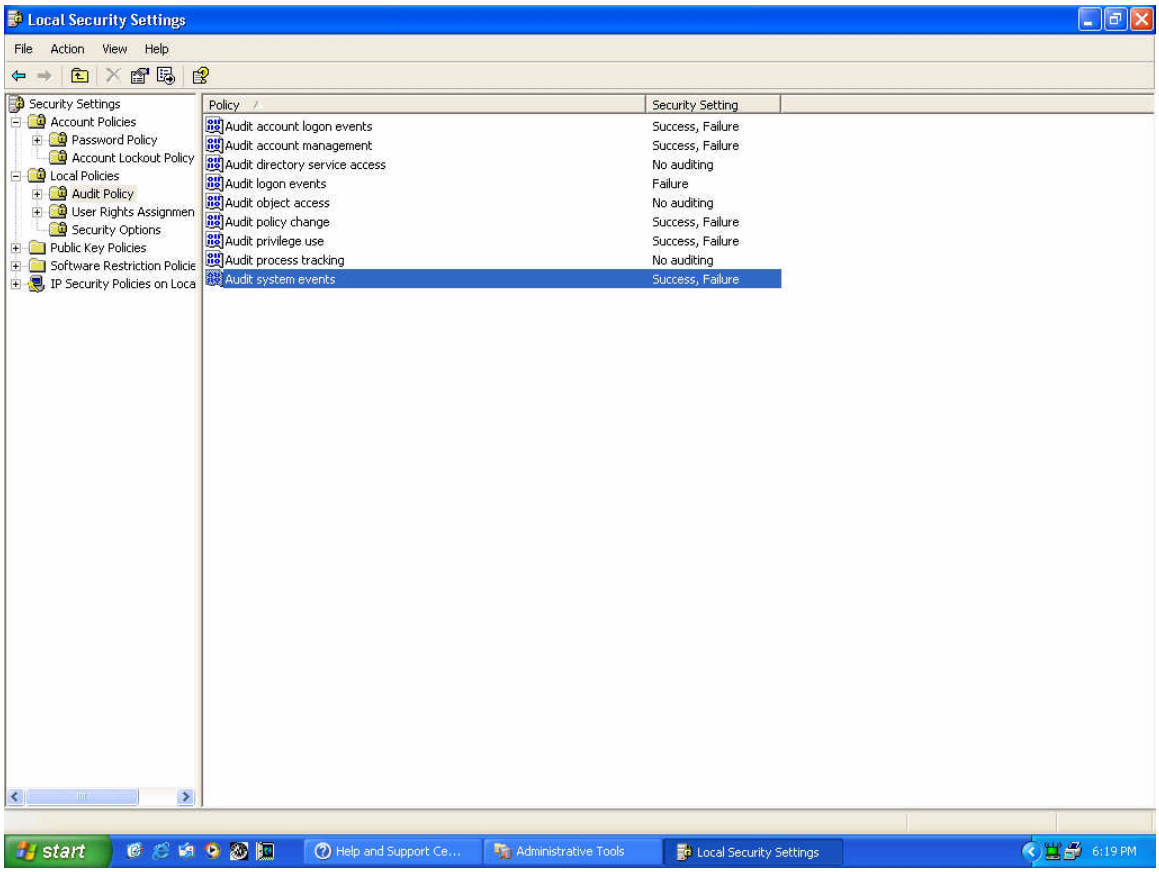
APPENDIX D.1 Password Policy



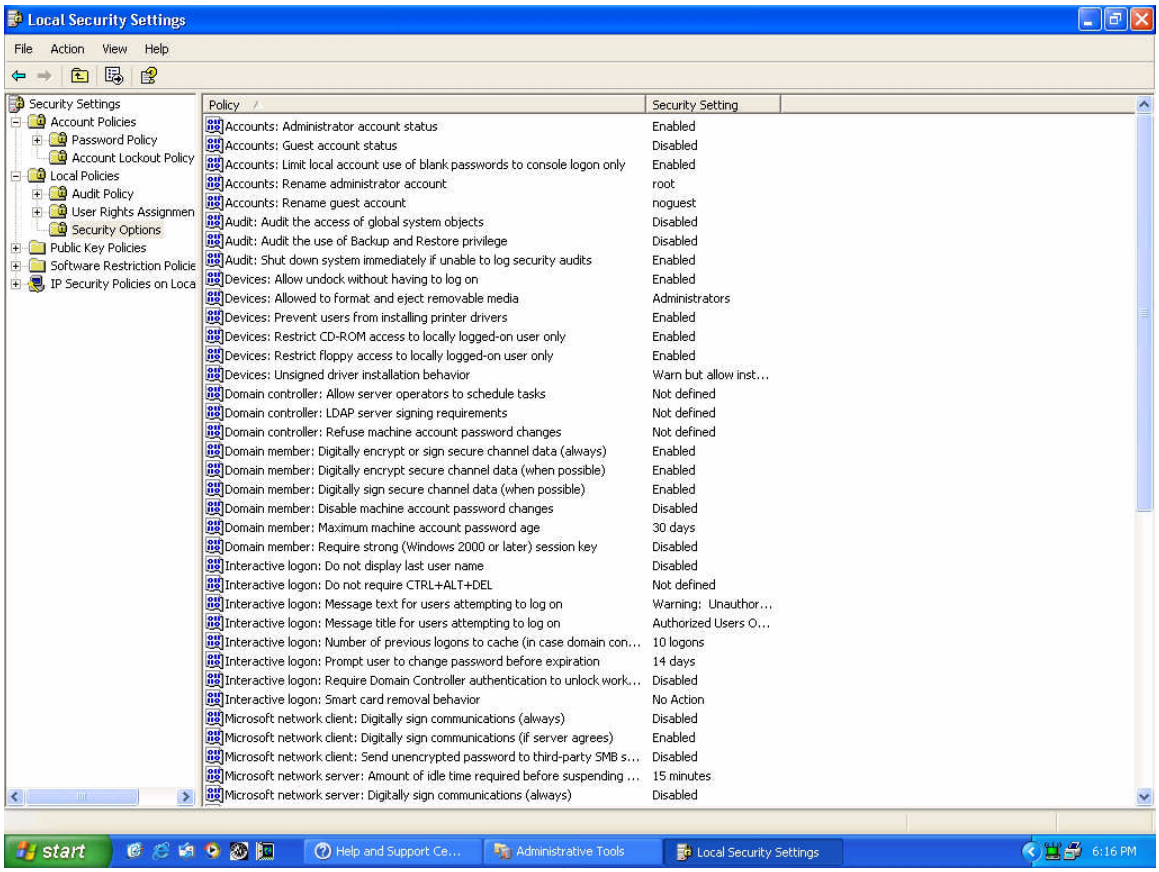
D.2 Account Lockout Policy



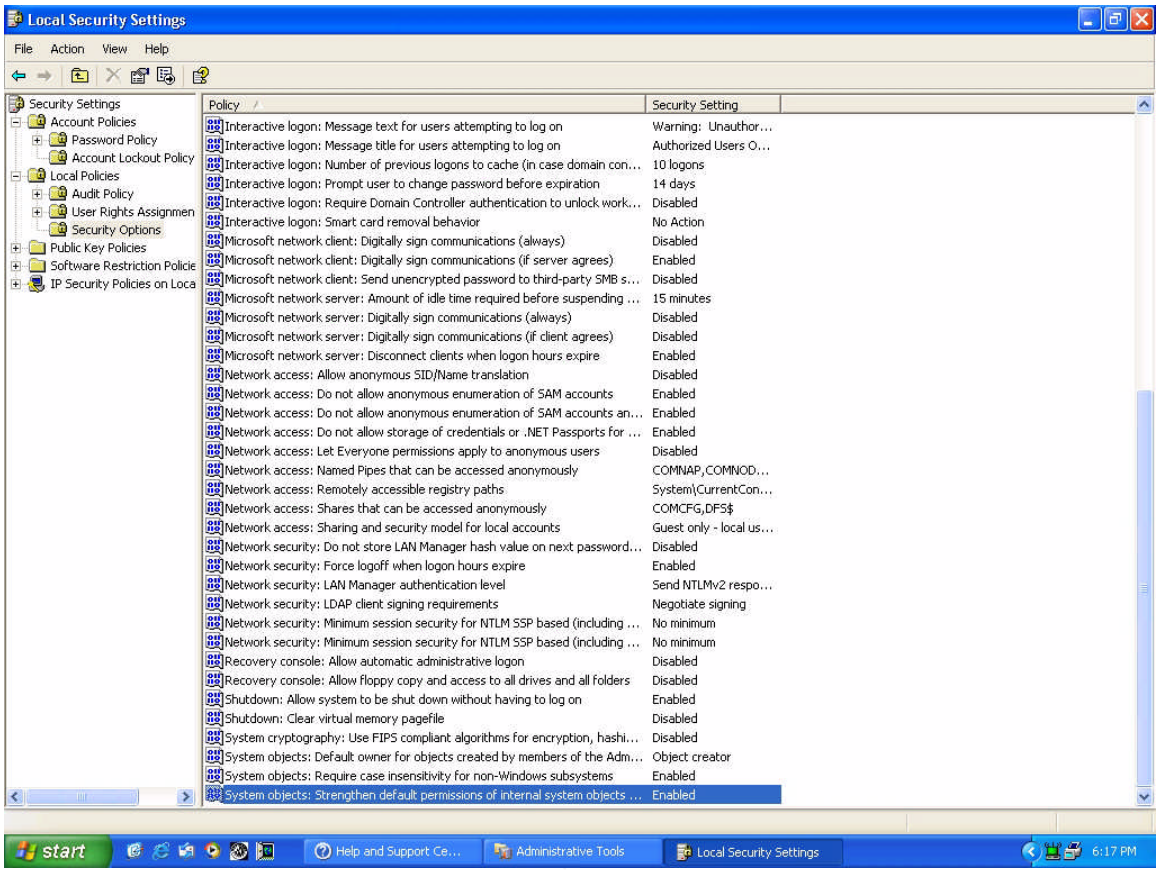
D.3 Audit Policy



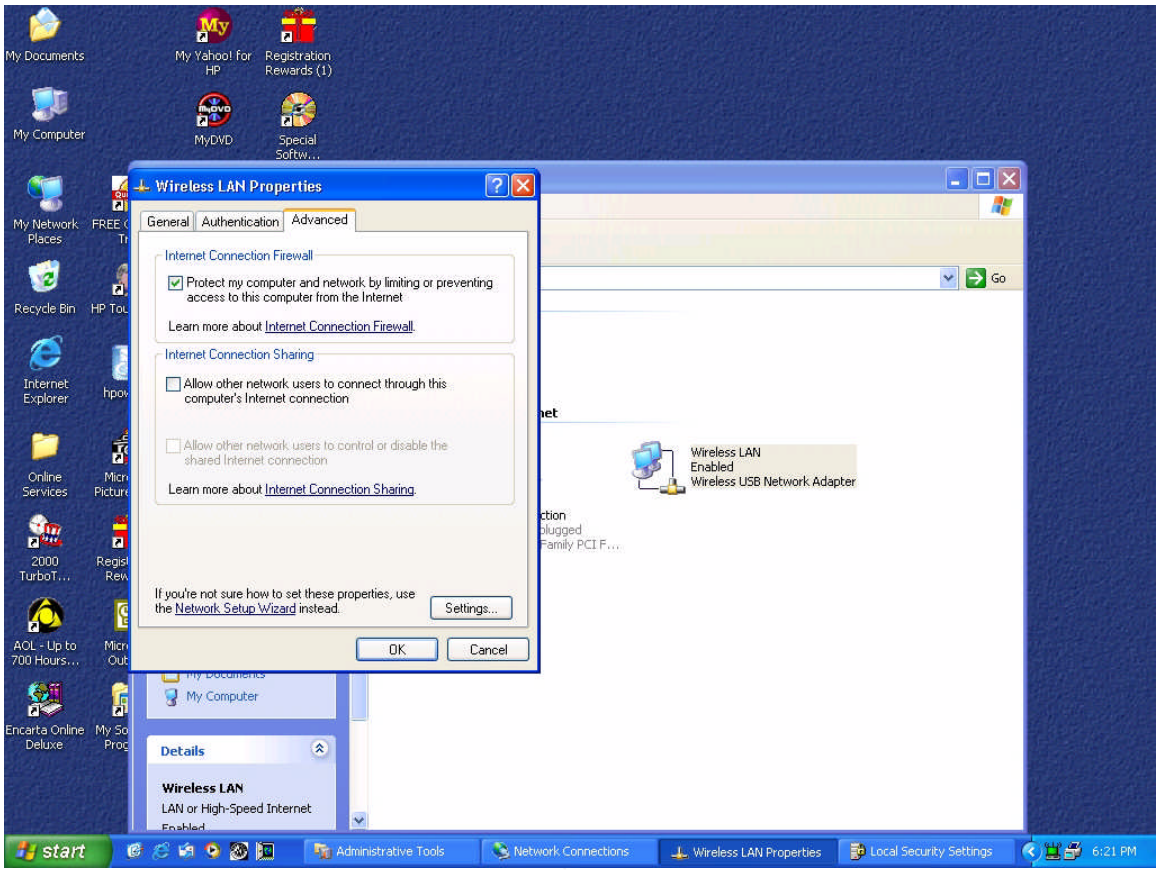
D.4.1 Security Options Page 1



D.4.2 Security Options Page 2



D.5 Internet Connection Firewall and Internet Connection Sharing



D.6.1 Nmap Output Default Installation

```
Starting nmap V. 2.54BETA26 ( www.insecure.org/nmap/ )
 Adding open port 445/tcp
 Adding open port 139/tcp
 Adding open port 5000/tcp
 Adding open port 135/tcp
Adding open port 1025/tcp
 Interesting ports on  (192.168.200.4):
(The 1543 ports scanned but not shown below are in state: closed)
Port       State       Service
135/tcp    open        loc-srv
139/tcp    open        netbios-ssn
445/tcp    open        microsoft-ds
1025/tcp   open        listen
5000/tcp   open        fics

Remote OS guesses: Windows Me or Windows 2000 RC1 through final
release, Windows Millenium Edition v4.90.3000

Nmap run completed -- 1 IP address (1 host up) scanned in 4 seconds
```

D.6.2 Nmap Output Post Install

```
Starting nmap V. 2.54BETA26 ( www.insecure.org/nmap/ )
 Warning:  OS detection will be MUCH less reliable because we did not
```

```
find at least 1 open and 1 closed TCP port
All 1548 scanned ports on  (192.168.200.4) are: filtered
Too many fingerprints match this host for me to give an accurate OS
guess
```

Nmap run completed -- 1 IP address (1 host up) scanned in 166 seconds

D.7 "Enum" Output

```
c:\tony\tools\enum\enum>enum -U -d -P -L -c 192.168.200.4

server: 192.168.200.4
setting up session... success.
couldn't get password policy
return 5, Access is denied.
couldn't get lockout policy
return 5, Access is denied.
opening lsa policy... success.
names:

c:\tony\tools\enum\enum\enum>
```

D.8 Audit Log (excerpt)

```
Type  Date  Time  Source      Category    Event User  Computer
Success Audit    11/30/2001  11:15:24 PM Security    System Event
      520   SYSTEM      MORNINGSTAR
Success Audit    11/30/2001  11:11:21 PM Security    Privilege Use
      577   howlett     MORNINGSTAR
Success Audit    11/30/2001  11:10:15 PM Security    Privilege Use
      577   howlett     MORNINGSTAR
Success Audit    11/30/2001  11:10:15 PM Security    Privilege Use
      577   howlett     MORNINGSTAR
Success Audit    11/30/2001  11:10:15 PM Security    Privilege Use
      577   howlett     MORNINGSTAR
Success Audit    11/30/2001  11:10:15 PM Security    Privilege Use
      577   howlett     MORNINGSTAR
Success Audit    11/30/2001  11:10:12 PM Security    Privilege Use
      576   howlett     MORNINGSTAR
Success Audit    11/30/2001  11:10:12 PM Security    Account Logon
      680   SYSTEM      MORNINGSTAR
Failure Audit    11/30/2001  11:10:03 PM Security    Logon/Logoff
      529   SYSTEM      MORNINGSTAR
Failure Audit    11/30/2001  11:10:03 PM Security    Account Logon
      680   SYSTEM      MORNINGSTAR
Failure Audit    11/30/2001  11:10:02 PM Security    Logon/Logoff
      535   SYSTEM      MORNINGSTAR
Failure Audit    11/30/2001  11:10:02 PM Security    Account Logon
      680   SYSTEM      MORNINGSTAR
Failure Audit    11/30/2001  11:10:02 PM Security    Logon/Logoff
      529   SYSTEM      MORNINGSTAR
Failure Audit    11/30/2001  11:10:02 PM Security    Account Logon
      680   SYSTEM      MORNINGSTAR
Success Audit    11/30/2001  11:10:02 PM Security    Privilege Use
      577   SYSTEM      MORNINGSTAR
Success Audit    11/30/2001  11:07:15 PM Security    Privilege Use
```

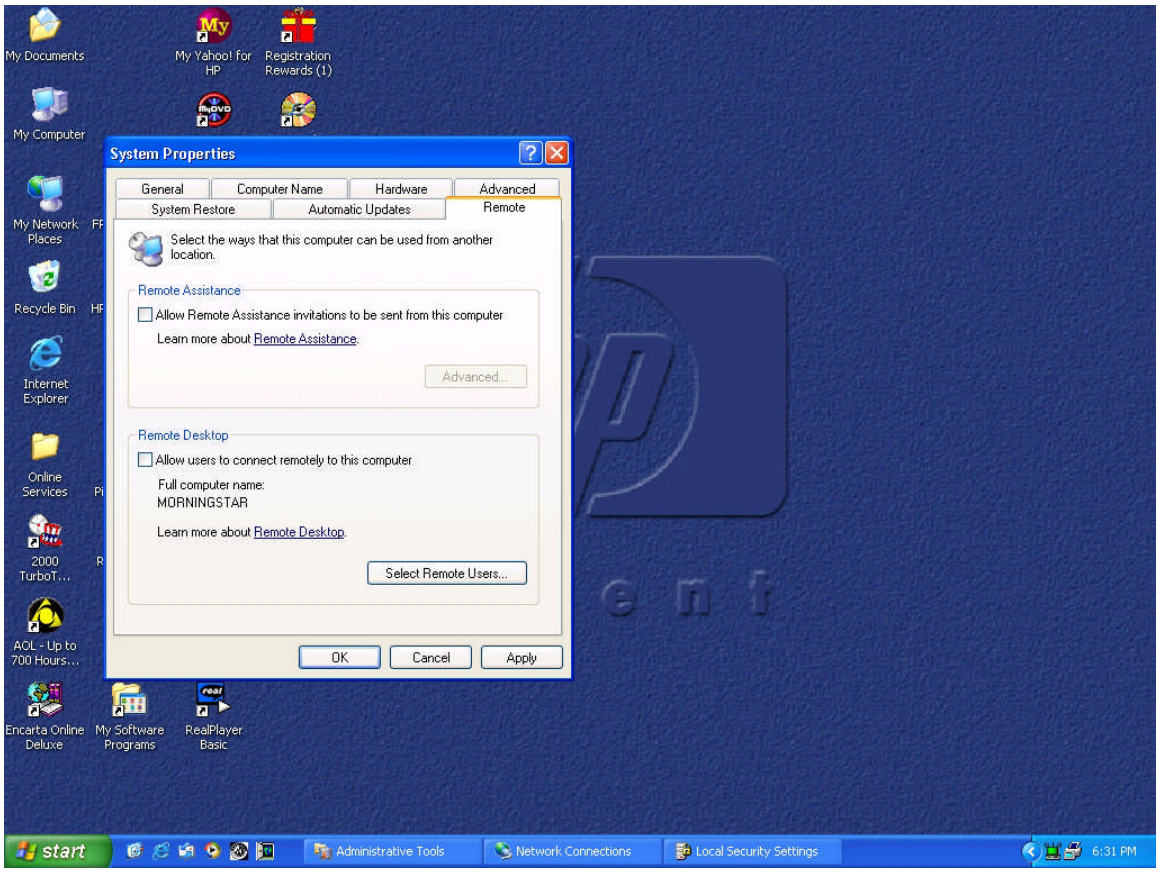
```
      577   SYSTEM      MORNINGSTAR
Success Audit    11/30/2001  11:07:14 PM Security   Privilege Use
      577   SYSTEM      MORNINGSTAR
Success Audit    11/30/2001  11:07:12 PM Security   Privilege Use
      576   LOCAL SERVICE    MORNINGSTAR
Success Audit    11/30/2001  11:07:08 PM Security   Privilege Use
      577   SYSTEM      MORNINGSTAR
Success Audit    11/30/2001  11:07:08 PM Security   System Event
      515   SYSTEM      MORNINGSTAR
Success Audit    11/30/2001  11:07:06 PM Security   System Event
      520   SYSTEM      MORNINGSTAR
Success Audit    11/30/2001  11:07:05 PM Security   System Event
      520   SYSTEM      MORNINGSTAR
Success Audit    11/30/2001  11:07:05 PM Security   System Event
      520   SYSTEM      MORNINGSTAR
Success Audit    11/30/2001  11:07:05 PM Security   Policy Change
      615   NETWORK SERVICE  MORNINGSTAR
Success Audit    11/30/2001  11:07:05 PM Security   Privilege Use
      576   LOCAL SERVICE    MORNINGSTAR
Success Audit    11/30/2001  11:07:05 PM Security   Privilege Use
      576   LOCAL SERVICE    MORNINGSTAR
Success Audit    11/30/2001  11:07:05 PM Security   Privilege Use
      576   LOCAL SERVICE    MORNINGSTAR
Success Audit    11/30/2001  11:07:05 PM Security   System Event
      515   SYSTEM      MORNINGSTAR
Success Audit    11/30/2001  11:07:05 PM Security   Privilege Use
      577   SYSTEM      MORNINGSTAR
Success Audit    11/30/2001  11:07:05 PM Security   System Event
      515   SYSTEM      MORNINGSTAR
Success Audit    11/30/2001  11:07:05 PM Security   Privilege Use
      577   SYSTEM      MORNINGSTAR
Success Audit    11/30/2001  11:07:05 PM Security   System Event
      515   SYSTEM      MORNINGSTAR
Success Audit    11/30/2001  11:07:04 PM Security   Privilege Use
      576   LOCAL SERVICE    MORNINGSTAR
Success Audit    11/30/2001  11:07:04 PM Security   Privilege Use
      577   SYSTEM      MORNINGSTAR
Success Audit    11/30/2001  11:07:04 PM Security   Privilege Use
      576   NETWORK SERVICE  MORNINGSTAR
Success Audit    11/30/2001  11:07:04 PM Security   Privilege Use
      577   SYSTEM      MORNINGSTAR
Success Audit    11/30/2001  11:07:04 PM Security   Privilege Use
      577   SYSTEM      MORNINGSTAR
Success Audit    11/30/2001  11:07:04 PM Security   Privilege Use
      577   SYSTEM      MORNINGSTAR
Success Audit    11/30/2001  11:07:04 PM Security   System Event
      518   SYSTEM      MORNINGSTAR
Success Audit    11/30/2001  11:07:04 PM Security   Privilege Use
      577   SYSTEM      MORNINGSTAR
Success Audit    11/30/2001  11:07:04 PM Security   Privilege Use
      577   SYSTEM      MORNINGSTAR
Success Audit    11/30/2001  11:07:04 PM Security   System Event
      515   SYSTEM      MORNINGSTAR
Success Audit    11/30/2001  11:07:04 PM Security   System Event
      515   SYSTEM      MORNINGSTAR
Success Audit    11/30/2001  11:07:04 PM Security   Privilege Use
      577   SYSTEM      MORNINGSTAR
Success Audit    11/30/2001  11:07:04 PM Security   System Event
```

```
      515   SYSTEM      MORNINGSTAR
Success Audit    11/30/2001  11:07:04 PM Security    System Event
      514   SYSTEM      MORNINGSTAR
Success Audit    11/30/2001  11:07:04 PM Security    System Event
      514   SYSTEM      MORNINGSTAR
Success Audit    11/30/2001  11:07:04 PM Security    System Event
      514   SYSTEM      MORNINGSTAR
Success Audit    11/30/2001  11:07:04 PM Security    System Event
      514   SYSTEM      MORNINGSTAR
Success Audit    11/30/2001  11:07:04 PM Security    System Event
      514   SYSTEM      MORNINGSTAR
Success Audit    11/30/2001  11:07:04 PM Security    System Event
      514   SYSTEM      MORNINGSTAR
Success Audit    11/30/2001  11:07:04 PM Security    System Event
      512   SYSTEM      MORNINGSTAR
Success Audit    11/30/2001  10:55:13 PM Security    Privilege Use
      578   howlett     MORNINGSTAR
Success Audit    11/30/2001  10:24:07 PM Security    Privilege Use
      578   howlett     MORNINGSTAR
Success Audit    11/30/2001  10:24:07 PM Security    Privilege Use
      578   howlett     MORNINGSTAR
Success Audit    11/30/2001  10:24:07 PM Security    Privilege Use
      578   howlett     MORNINGSTAR
Success Audit    11/30/2001  9:56:47 PM  Security    Privilege Use
      576   howlett     MORNINGSTAR
Success Audit    11/30/2001  9:56:47 PM  Security    Account Logon
      680   SYSTEM      MORNINGSTAR
Failure Audit    11/30/2001  9:56:38 PM  Security    Logon/Logoff
      529   SYSTEM      MORNINGSTAR
Failure Audit    11/30/2001  9:56:38 PM  Security    Account Logon
      680   SYSTEM      MORNINGSTAR
Failure Audit    11/30/2001  9:56:22 PM  Security    Logon/Logoff
      529   SYSTEM      MORNINGSTAR
Failure Audit    11/30/2001  9:56:22 PM  Security    Account Logon
      680   SYSTEM      MORNINGSTAR
Failure Audit    11/30/2001  9:56:18 PM  Security    Logon/Logoff
      529   SYSTEM      MORNINGSTAR
Failure Audit    11/30/2001  9:56:18 PM  Security    Account Logon
      680   SYSTEM      MORNINGSTAR
Failure Audit    11/30/2001  9:56:09 PM  Security    Logon/Logoff
      529   SYSTEM      MORNINGSTAR
Failure Audit    11/30/2001  9:56:09 PM  Security    Account Logon
      680   SYSTEM      MORNINGSTAR
Failure Audit    11/30/2001  9:56:09 PM  Security    Logon/Logoff
      535   SYSTEM      MORNINGSTAR
Failure Audit    11/30/2001  9:56:09 PM  Security    Account Logon
      680   SYSTEM      MORNINGSTAR
Failure Audit    11/30/2001  9:56:09 PM  Security    Logon/Logoff
      529   SYSTEM      MORNINGSTAR
Failure Audit    11/30/2001  9:56:09 PM  Security    Account Logon
      680   SYSTEM      MORNINGSTAR
Success Audit    11/30/2001  7:44:30 PM  Security    System Event
      520   SYSTEM      MORNINGSTAR
Failure Audit    11/30/2001  7:44:26 PM  Security    Policy Change
      615   NETWORK SERVICE   MORNINGSTAR
Success Audit    11/30/2001  7:44:26 PM  Security    System Event
```

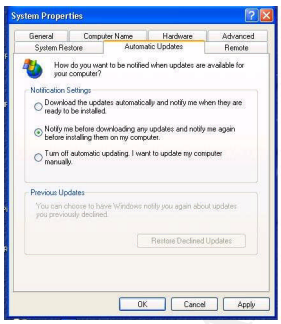
```
      520   SYSTEM      MORNINGSTAR
Success Audit    11/30/2001  7:29:28 PM  Security    Privilege Use
      577   SYSTEM      MORNINGSTAR
Success Audit    11/30/2001  7:29:27 PM  Security    Privilege Use
      577   SYSTEM      MORNINGSTAR
Failure Audit    11/30/2001  6:42:32 PM  Security    Logon/Logoff
      535   SYSTEM      MORNINGSTAR
Failure Audit    11/30/2001  6:42:32 PM  Security    Account Logon
      680   SYSTEM      MORNINGSTAR
Failure Audit    11/30/2001  6:42:32 PM  Security    Logon/Logoff
      529   SYSTEM      MORNINGSTAR
Failure Audit    11/30/2001  6:42:32 PM  Security    Account Logon
      680   SYSTEM      MORNINGSTAR
Failure Audit    11/30/2001  6:42:32 PM  Security    Logon/Logoff
      529   SYSTEM      MORNINGSTAR
Failure Audit    11/30/2001  6:42:32 PM  Security    Account Logon
      680   SYSTEM      MORNINGSTAR
Success Audit    11/30/2001  6:42:25 PM  Security    Account
Management  628   howlett     MORNINGSTAR
Failure Audit    11/30/2001  6:41:30 PM  Security    Logon/Logoff
      535   SYSTEM      MORNINGSTAR
Failure Audit    11/30/2001  6:41:30 PM  Security    Account Logon
      680   SYSTEM      MORNINGSTAR
Success Audit    11/30/2001  6:41:30 PM  Security    Account
Management  642   howlett     MORNINGSTAR
Success Audit    11/30/2001  6:41:30 PM  Security    Account
Management  636   howlett     MORNINGSTAR
Success Audit    11/30/2001  6:41:29 PM  Security    Account
Management  642   howlett     MORNINGSTAR
Success Audit    11/30/2001  6:41:29 PM  Security    Account
Management  626   howlett     MORNINGSTAR
Success Audit    11/30/2001  6:41:29 PM  Security    Account
Management  624   howlett     MORNINGSTAR
Success Audit    11/30/2001  6:41:29 PM  Security    Account
Management  632   howlett     MORNINGSTAR
Success Audit    11/30/2001  6:41:29 PM  Security    Account
Management  630   howlett     MORNINGSTAR
Success Audit    11/30/2001  6:41:29 PM  Security    Account
Management  633   howlett     MORNINGSTAR
Success Audit    11/30/2001  6:41:29 PM  Security    Account
Management  624   howlett     MORNINGSTAR
Success Audit    11/30/2001  6:41:29 PM  Security    Account
Management  632   howlett     MORNINGSTAR
Failure Audit    11/30/2001  6:41:06 PM  Security    Logon/Logoff
      529   SYSTEM      MORNINGSTAR
Failure Audit    11/30/2001  6:41:06 PM  Security    Account Logon
      680   SYSTEM      MORNINGSTAR
Failure Audit    11/30/2001  6:41:06 PM  Security    Logon/Logoff
      529   SYSTEM      MORNINGSTAR
Failure Audit    11/30/2001  6:41:06 PM  Security    Account Logon
      680   SYSTEM      MORNINGSTAR
Failure Audit    11/30/2001  6:35:50 PM  Security    Logon/Logoff
      529   SYSTEM      MORNINGSTAR
Failure Audit    11/30/2001  6:35:50 PM  Security    Account Logon
      680   SYSTEM      MORNINGSTAR
Failure Audit    11/30/2001  6:35:50 PM  Security    Logon/Logoff
      529   SYSTEM      MORNINGSTAR
Failure Audit    11/30/2001  6:35:50 PM  Security    Account Logon
```

```
      680   SYSTEM      MORNINGSTAR
Success Audit    11/30/2001  6:35:26 PM  Security   Privilege Use
      578   howlett     MORNINGSTAR
Success Audit    11/30/2001  6:35:26 PM  Security   Privilege Use
      578   howlett     MORNINGSTAR
Success Audit    11/30/2001  6:31:04 PM  Security   Privilege Use
      576   NETWORK SERVICE  MORNINGSTAR
Success Audit    11/30/2001  6:31:03 PM  Security   Privilege Use
      578   howlett     MORNINGSTAR
Success Audit    11/30/2001  6:31:03 PM  Security   Privilege Use
      578   howlett     MORNINGSTAR
Success Audit    11/30/2001  6:31:03 PM  Security   Privilege Use
      578   howlett     MORNINGSTAR
Success Audit    11/30/2001  6:31:03 PM  Security   Privilege Use
      578   howlett     MORNINGSTAR
Success Audit    11/30/2001  6:31:03 PM  Security   Privilege Use
      578   howlett     MORNINGSTAR
Success Audit    11/30/2001  6:31:03 PM  Security   Privilege Use
      578   howlett     MORNINGSTAR
Success Audit    11/30/2001  6:31:03 PM  Security   Privilege Use
      578   howlett     MORNINGSTAR
Success Audit    11/30/2001  6:31:03 PM  Security   Privilege Use
      578   howlett     MORNINGSTAR
Success Audit    11/30/2001  6:31:03 PM  Security   Privilege Use
      578   howlett     MORNINGSTAR
Success Audit    11/30/2001  6:31:03 PM  Security   Privilege Use
      578   howlett     MORNINGSTAR
Success Audit    11/30/2001  6:31:03 PM  Security   Privilege Use
      578   howlett     MORNINGSTAR
Success Audit    11/30/2001  6:31:03 PM  Security   Privilege Use
      578   howlett     MORNINGSTAR
Success Audit    11/30/2001  6:31:03 PM  Security   Privilege Use
      578   howlett     MORNINGSTAR
Success Audit    11/30/2001  6:31:03 PM  Security   Privilege Use
      578   howlett     MORNINGSTAR
Success Audit    11/30/2001  6:31:03 PM  Security   Privilege Use
      578   howlett     MORNINGSTAR
Success Audit    11/30/2001  6:30:10 PM  Security   Privilege Use
      576   LOCAL SERVICE    MORNINGSTAR
Success Audit    11/30/2001  6:19:01 PM  Security   Policy Change
      612   howlett     MORNINGSTAR
Success Audit    11/30/2001  6:18:53 PM  Security   Policy Change
      612   howlett     MORNINGSTAR
Success Audit    11/30/2001  6:18:47 PM  Security   Policy Change
      612   howlett     MORNINGSTAR
```

D.9 Remote Assist



D.9.1 Autoupdate Settings



D.10 Users Accounts