GSNA Practical v4.0

Option 1, Topic 2

Baselining a Windows 2000 Professional Computer System

Robert L. Fanelli
March 25, 2005

ABSTRACT

This paper details the rationale and procedures for baselining a Windows 2000 Professional computer system. The goal is to provide a set of efficient and effective procedures and to use only publicly available tools. The paper describes the system in question and the elements of the baseline. It then discusses the procedures for establishing the baseline and significance of the elements included. Finally, the paper discusses the procedure for evaluating systems against the baseline and the significance of the results.

TABLE OF CONTENTS

INTRODUCTION

We establish a baseline to provide a point of reference for evaluating the security and integrity of a system. The baseline gives us a picture of what 'right' looks like for a given system.

This paper lays out a comprehensive procedure for establishing a baseline for a Windows 2000 Professional computer system and evaluating systems against that baseline. There are several methods and commercial products for baselining. This paper presents a baselining procedure intended to be easy to use and low-cost, using only freely available tools.

SECTION 1 : IDENTIFY THE BASELINE

1.1 Description of the System.

The system is a stand-alone, notebook computer. This system is primarily used for basic computing and communications by members of the organization during travel or telecommuting. The system operates outside the organization's security perimeter, frequently on untrustworthy networks such as a residential broadband service or hotel in-room LAN.

Interface with internal organizational services, such as electronic mail, is via web-enabled applications secured with Secure Sockets Layer (SSL). The system provides basic application support and is configured to provide a reasonable mix of security and reliability for the user.

Our baseline deals with three main areas: the operating system, the installed software and the security configuration settings for the system. We use a standard hardware platform with the hard drive on each system imaged from a trusted master image. After imaging, system-unique settings such as host name and local user accounts are applied manually.

1.2 Hardware.

The hardware is a Dell Latitude C840 notebook computer. The CPU is a 2.4 GHz Pentium 4 Processor. The system has 1GB of RAM. The device includes a 60GB hard disk drive, an integral DVD/CD-RW drive and a modular floppy disk drive. The modular floppy drive may be replaced with a secondary battery or an optical drive. The system has an integral 10/100Mb/s network interface and a V.92 modem. System interfaces include two USB

2.0 ports, digital video out, S-video out, serial, parallel, a single PS/2 mouse/keyboard port, PCMCIA, firewire and infrared (IR) port. The system includes both touchpad and 'mouse stick' interfaces.

The organizational security policy does not allow the use of wireless network interfaces. This system has neither a PCMCIA wireless NIC nor integrated wireless capability (e.g. Centrino). Additionally, the IR port is disabled by the simple expedient of placing an IR-opaque sticker over the port.

1.3 Operating system.

The system runs on the Microsoft Windows 2000 Professional operating system with Service Pack 4. Operating system updates and hotfixes are applied in accordance with organizational policy. The organization tests all updates prior to incorporating them into the baseline and deploying them to production systems.

Windows 2000 Professional provides a robust set of capabilities for securing a system. Unfortunately, the default configuration of Windows 2000 'out of the box' emphasizes usability and compatibility over security. However, with a little work, a knowledgeable administrator can make a Windows 2000 system quite secure while retaining usability.

Windows 2000 Professional offers the benefits of a 'mature' operating system. Many of the security issues have been identified and corrected over time. The interaction of our application software with this operating system is well known. The years of experience that the organization's IT personnel have with this operating system improves our security posture. The IT personnel are thoroughly familiar with the Windows 2000 security settings and understand the security ramifications of their actions.

The NT File System (NTFS) provides fine-grained access controls and auditing capabilities. Additionally, Windows 2000 offers an Encrypting File System (EFS) to protect the confidentiality of information stored in an NTFS volume. While EFS cannot defeat a determined attacker, it does provide an extra measure of protection from data theft by a less capable or less determined individual.

1.4 Installed Software.

The baseline includes a standard set of productivity applications, drivers and security software. The baseline includes the following installed software:

Microsoft Internet Explorer 6 with SP1
Microsoft Office 2000 SR1 Professional with Service Pack 3 and patches. The installed office applications are:

Microsoft Word
Microsoft PowerPoint

Microsoft Excel
Microsoft Access
Microsoft Outlook 2000
Microsoft Photo Editor
Microsoft Binder

Windows Media Player 9
Adobe Acrobat Reader 6.0.1
WinZip 8.0
InterVideo WinDVD
Roxio Easy CD Creator 5 Basic
Microsoft Baseline Security Analyzer 1.2.1

Drivers installed:
ALPS Touch Pad Driver
Intel SpeedStep technology Applet
NVIDIA Windows 2000/XP Display Drivers
PCTEL 2304WT V.92 MDC Modem Drivers

Symantec Client Security with:
Symantec Antivirus Version 9.0.0.338
Symantec Client Firewall Version 7.1.0.98
Live Update 2.0

Having accountability for the software installed on the system is a critical part of the baseline. We cannot effectively monitor the integrity of the system unless we know what software is supposed to be present. This is both a restrictive and permissive measure; we want to ensure no extraneous software is loaded as well as ensure that the software we expect, especially the security software, has not been removed.

1.5 Security Configuration.

Specifying the operating system and application software is not enough. As mentioned above, the Windows 2000 default configuration is not secure. Fortunately, Windows 2000 provides tools to easily lock the system down. This is a critical part of ensuring the system's security posture. These settings allow us to make our Windows 2000 system acceptably secure. This is also an important part of the baseline because changes to the security configuration may indicate potential exposures and they may also provide evidence of other security issues. The auditor must not only ask the question "what effect does this change have on security?" he must also ask "who or what changed this and how?"

The organization has a baseline of security configuration settings that complement the organizational security policy. The organizational policy for Windows 2000 is derived in large part from NIST recommendations [Souppaya 02]. These settings have been codified in a Windows 2000 security template.

This template was derived from the Windows 2000 Gold Standard Security Template, a joint effort of SANS, the National Institute of Standards and Technology (NIST), the National Security Agency (NSA), the Defense Information Systems Agency (DISA) and the Center for Internet Security (CIS). [Bower02] The organizational template has certain differences from the Gold Standard template in order to adhere to the organizational security policy and to ensure required system functionality.

The Symantec Client Security products are configured to operate in a stand-alone mode in an untrusted network environment. The settings are imported into Symantec Client Security from an organizational standard configuration file. The Symantec client software runs in the unmanaged mode, with daily signature updates and weekly antivirus scans enabled. The intent of this policy is to make security 'easy' for the end user.

This software is critical to ensuring the security of our stand-alone system. The client firewall not only provides a robust means for keeping network intruders out, it also provides warning that potentially malicious software on the system is trying to get out. The antivirus software is essential, not only to protecting the user, but also to ensuring the system does not become a host for malicious software and a threat to others on the network.

SECTION 2 : DEVELOP THE BASELINE

2.1 Overview.

This section describes the development of the baseline. First, we will present an overview of the process of building the baseline system. Then we will cover the process of mapping the file system, setting and recording the security configuration and taking and inventory of the installed software.

2.2 Creating The Baseline System Image.

We will not go into great detail on the procedures for creating a Windows 2000 Professional system image. A short guide to the process is provided at [Microsoft00]. Several other references are also available.

First, we ‘burn the system to the ground’. We overwrite the manufacturer hard drive image, reformatting the hard drive and installing the operating system from trusted media. Application software is also installed from trusted media.

The operating system and all installed applications are updated to the level approved by the organization. As of this writing, all existing patches for Windows 2000, Microsoft Office 2000 and the other installed applications were approved for deployment. Thus, this baseline should show no discrepancies between installed patches and those available in the Microsoft Windows Update Catalog.

After the operating system and application software are installed, we apply the organizational security template. A template can be applied either through the Microsoft Management Console (MMC) Security Template snap-in or using SECEDIT from the command line. In this case we apply the template from trusted media using SECEDIT:

```
C:\> secedit /configure /DB C:\WINNT\security\Database\orgsecedit.sdb /CFG
A:\orgtemplate.inf /verbose
```

This creates a new security database called 'orgsecedit.sdb' from the settings in 'orgtemplate.inf' and applies it as the system's current security configuration. A tutorial on the use of SECEDIT is available in [Bower02 pp36-38].

2.3 Baseline File System Map.

The first step to recording the system baseline is to map the file system. We are primarily interested in detecting changes to the executable files (e.g. .exe and .dll) in the file system and to other key operating system files. Malicious software will typically modify existing executables or introduce new ones. Some of the most serious compromises involve subversion of the operating system itself by a ‘root kit’ or ‘admin kit’. Information is available at [Cogswell05].

We are not particularly interested in monitoring files such as user content, logs, web browser cache and so on. These files change routinely and do not pose a significant risk to a well-secured system. These files are not part of the baseline.

The open-source FTimes (File Topography and Integrity Monitoring on an Enterprise Scale) tool will capture and compare our file system maps. [http://ftimes.sourceforge.net/FTimes/index.shtml] FTimes produces a map file containing a fingerprint for each item in the file system, or a portion of the file system. FTimes examines each file and collects the following data elements:

From the FTimes Man Page: [Monroe04]

volume	- Volume serial number
findex	- File serial number
attributes	- File attributes
atime	- Time of last file access
mtime	- Time of last file modification
ctime	- Creation time

chtime - Change time (undocumented)
size - File size in bytes
altstreams - Number of alternate or named streams
magic - File type
md5 - MD5 digest of the file's data stream

The MD5 digest is especially important. Any alteration in the file data will alter this value. Some malicious software can alter or replace legitimate files while keeping values like the file size the same. Given the one-way function nature of the MD5, it is infeasible to create a file that will produce an identical MD5 sum to another file. Thus, this serves as a unique 'fingerprint' for each file.

We use the 'alternate operating system' baseline technique, as discussed in [Monroe02 pp5-6]. The alternate operating system method has the advantage of giving an 'out of band' [Monroe02 p5] view of the files on the hard drive. If the operating system is compromised by malicious software such as a rootkit, the view of the files could be inacurate. This type of software can alter the operating system, causing it to lie to us and to hide suspicious files. Another possibility is that even an uncompromised operating system can lock or hide some files, preventing a tool from mapping them accurately from within. Booting up under an alternate operating system, located on a separate drive, gives us an unrestricted view of the entire NTFS volume.

A fairly easy and unobtrusive way of baselining with an alternate operating system is to boot the system into Linux using a 'live CD'. This is a complete, functional operating system contained on a bootable CD. For this process, we are using the Knoppix Security Tools Distribution [http://www.knoppix-std.org/]. This is a Knoppix live Linux distribution optimized for security practitioners. It includes several useful tools; among them is FTimes.

We use a USB ‘Thumb Drive’ to hold the necessary configuration files and to store the results from our baselining tools. It is possible to accomplish these tasks using the network interface. However, using the USB drive allows us to keep the system isolated from the network. This is especially important later on, when we are evaluating system integrity against the baseline. This it an important step to allowing an ‘outside’ system to attached to the organizational network. Thus, we need a technique that allows us to work with a stand-alone system.

File System Mapping Procedure.

1) Boot the system using the Knoppix STD CD:
-Power the system on and press F12 for the boot menu.
-Insert the CD into the drive and select it as the boot device
-At the boot prompt, enter 'fb1024x768' to get a readable display

2) Mount the drives:

-Right click on the desktop

-Select 'Forensics' from the context menu and then 'Forensics Shell' from the forensics menu.

-Mount the NTFS volume read-only. At the command line:

```
root@1[forensics]# mount -r -t ntfs  /dev/hda1 /mnt/hda1
```

-Insert the USB drive into the USB port and mount it as a MS DOS volume:

```
root@1[forensics]# mount -t msdos /dev/sda1 /mnt/sda1
```

3) Start the FTimes map process:

```
root@1[forensics]# ftimes --mapfull /mnt/sda1/baseline.cfg
```

This invokes the mapfull function of FTimes to produce a file system map, using the configuration settings in baseline.cfg on the USB drive.

The baseline.cfg has the following entries:

```
BaseName=C840
OutDir=/mnt/sda1/
RunType=baseline
FieldMask=NONE+mtime+size+md5
Include=/mnt/hda1
Exclude=/mnt/hda1/Documents and Settings
```

BaseName=C840 : This arbitrary string specifies the first portion of the output filename. The date and time of the operation will be appended to this to generate the filename.

OutDir=/mnt/sda1/ : Specifies the directory for the output, in this case the USB drive. The output is a map file with a .map extension and a log file with a .log extension.

RunType=baseline : Marks the map file as a baseline rather than an operational snapshot.

FieldMask=NONE+mtime+size+md5 : Specifies the fields we wish to include in the map. In this case we include the last time the file was modified, the file size and the MD5 value for the file. Since we are primarily interested in detecting changes, these fields are more than sufficient.

Include=/mnt/hda1 : Include the entire NTFS volume, mounted at /mnt/hda1, in the map.

Exclude=/mnt/hda1/Documents and Settings : Exclude the 'Documents and Settings' sub-tree from the map. This sub-tree does not contain any critical operating system or application software files. However, it does include a large amount of user documents, web browser cache, etc. that change frequently without compromising security. Excluding this from the map reduces the 'background noise' when evaluating a snapshot against the baseline map.

Maping the file system with this configuration takes 20-25 minutes. The map file and log are written to the USB drive. We will burn a copy of this file to CD-R to act as a read-only reference copy for the baseline. The log file includes a MD5 value for the entire map file. We record this value to hardcopy so we can confirm the integrity of the map file, as required.

An extract of the map file is in Appendix 2. The entire file is close to 2MB in size and would cover over 125 printed pages.

2.4 The Organizational Security Template.

Our organizational security template acts as a set of expected values for our security settings. In section 2.2 above, we discussed applying this template to the baseline system as part of the initial build. The expected value for these setting is that same as the setting in the organizational security template.

The security configuration is at least as important as the installed operating system and software in determining the overall security posture of the system. Even if the system is well patched and is free of problem software, it will still be vulnerable if it is not configured to be secure. Microsoft Windows 2000 Professional requires a significant amount of alteration from the default configuration in order to be reasonably secure. Fortunately, the OS provides robust tools to do this security configuration. Furthermore, sample security templates and documents detailing best practices for securing Windows 2000 are readily available from multiple sources.

The organization's baseline security configuration for this system is codified in a Windows 2000 security template. We use the organization's security template as a baseline control for the system's security configuration. The template is useful, not only as a means to rapidly configure the security settings on the baseline system, but also for efficiently comparing the security configuration on a production system against the baseline.

A security template is a text file containing specifically formatted security settings. For the most part, the file is a set of registry settings and reads much like a file containing exported registry settings. The template can specify any of the security settings available in the 'Local Security Policy' administrative tool plus several others. It can also set access controls on files and directories in an NTFS volume and on objects in the registry. A detailed discussion of creating and using Windows 2000 security templates can be found in [Bower02] and [Microsoft03]

A caution in using templates: there is no 'undo' function. Applying another template does not necessarily remove the effects of a previous template. Each value must be specifically addressed by the template being applied, or it is not changed. Making backups of the registry and the security database are helpful in rolling back from a bad security template. It is imperative to thoroughly test these settings before deploying to production systems; it is quite easy to break things in subtle ways.

The security template is Appendix 1.

2.5 Additional Configuration Items.

A few security-related configuration settings are not readily set or evaluated with security templates. These are fall into two areas. First are settings related to the operating system and the installed Microsoft application software. Second are the settings related to the installed Symantec Client Security suite.

For the Symantec product, we will manually examine critical settings to ensure the software is protecting the system. Details of this process are below.

For the operating system and Microsoft software we are primarily interested in items such as account administration, software updates and application security settings. We will use the Microsoft Baseline Security Analyzer (MBSA) V1.2.1 to capture a report of these settings from the baseline system. We can then compare this baseline report to MBSA reports from production systems to efficiently evaluate their compliance with the baseline.

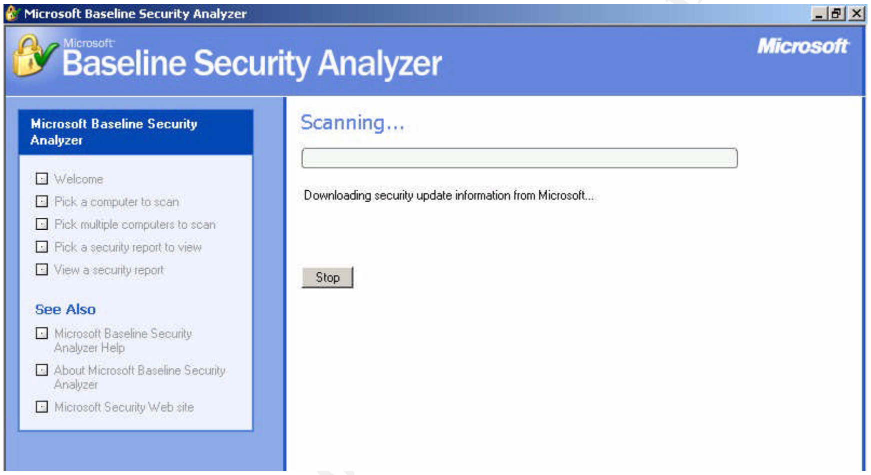
The Microsoft Baseline Security Analyzer is an easy to use tool, available at no cost from Microsoft. This tool is useful for getting a system into a secure state during the initial build and for evaluating the state of security later. A discussion on MBSA is in [Microsoft04].

MBSA is available as a no-cost download from Microsoft.
[http://www.microsoft.com/technet/security/tools/mbsahome.mspx]
We have downloaded it and installed it as a part of our system baseline. It is possible for MBSA to scan a system across the network, but we have opted to install the application locally to support stand-alone operations.

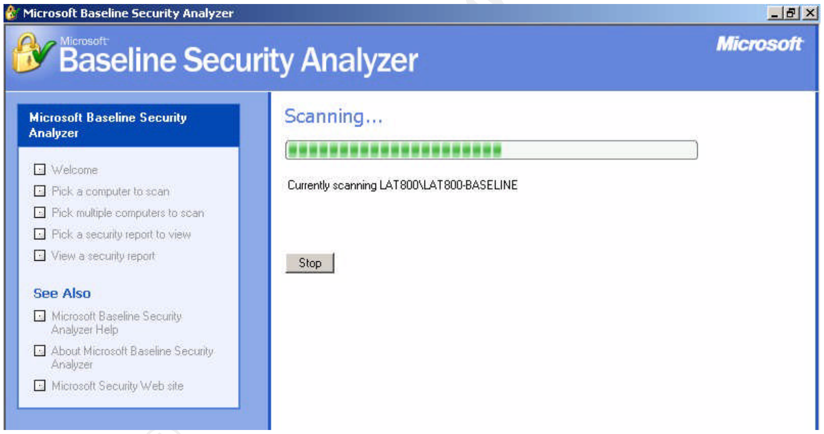
We use a trusted workstation with MBSA installed to hold the MBSA reports from our baseline system and any production systems we test. For stand alone systems, we move the reports into this machine using the USB drive. The

reports default to:
C:\Documents and Settings\<UserName>\SecurityScans\<Domain-MachineName-DateTime>.xml
Reports copied onto the machine will appear in the list of available reports.

To create the baseline report, start the program and click "Scan a computer". On the "Pick a Computer to Scan" page, click "Start scan"; MBSA defaults to scanning the local machine only. MBSA will attempt to connect to Microsoft to download an updated copy of the security database file, mssecure.xml. We can either allow this machine an external network connection to get the update or manually transfer an updated copy of mssecure.xml from the MSBA installation on another machine. The default installation path is "*C:\Program Files\Microsoft Baseline Security Analyzer\mssecure.xml*".


Microsoft Baseline Security Analyzer
Microsoft
Baseline Security Analyzer
Microsoft
Microsoft Baseline Security Analyzer
Welcome
Pick a computer to scan
Pick multiple computers to scan
Pick a security report to view
View a security report
See Also
Microsoft Baseline Security Analyzer Help
About Microsoft Baseline Security Analyzer
Microsoft Security Web site
Scanning...
Stop

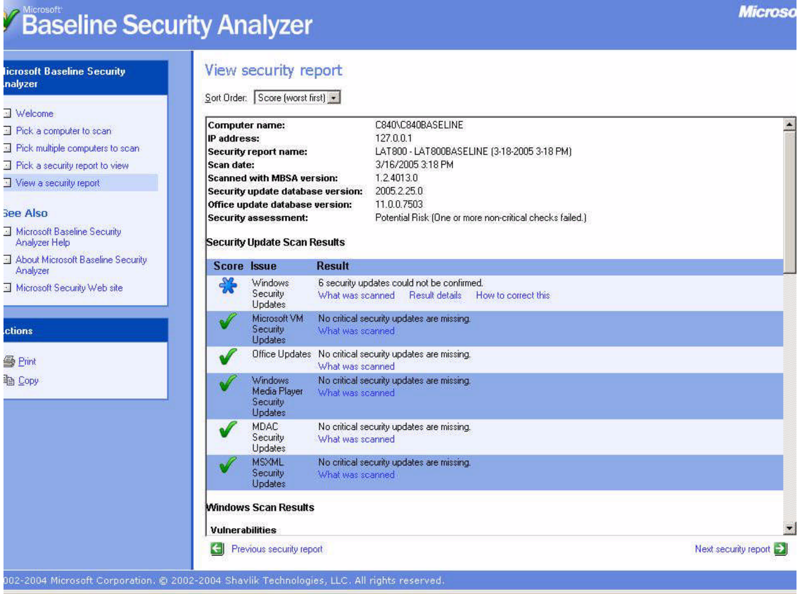
Downloading security update information from Microsoft...


Microsoft Baseline Security Analyzer
Microsoft
Baseline Security Analyzer
Microsoft
Microsoft Baseline Security Analyzer
Welcome
Pick a computer to scan
Pick multiple computers to scan
Pick a security report to view
View a security report
See Also
Microsoft Baseline Security Analyzer Help
About Microsoft Baseline Security Analyzer
Microsoft Security Web site
Scanning...
Stop

Currently scanning LAT800\LAT800-BASELINE

Even if it cannot connect to Microsoft for an update, MBSA will still perform the system scan. However, the results, especially for updates, may be inaccurate if an old security database is used.

At the conclusion of the scan, the MBSA report is displayed.


Microsoft Baseline Security Analyzer
Microso
icrosoft Baseline Security
nalyzer
Welcome
Pick a computer to scan
Pick multiple computers to scan
Pick a security report to view
View a security report
See Also
Microsoft Baseline Security Analyzer Help
About Microsoft Baseline Security Analyzer
Microsoft Security Web site
ctions
Print
Copy
Previous security report
Next security report
002-2004 Microsoft Corporation. © 2002-2004 Shavlik Technologies, LLC. All rights reserved.

View security report

Sort Order: Score (worst first)

Computer name:	C840\C840BASELINE
IP address:	127.0.0.1
Security report name:	LAT800 - LAT800BASELINE (3-18-2005 3-18 PM)
Scan date:	3/16/2005 3:18 PM
Scanned with MBSA version:	1.2.4013.0
Security update database version:	2005.2.25.0
Office update database version:	11.0.0.7503
Security assessment:	Potential Risk (One or more non-critical checks failed.)

Security Update Scan Results

Score	Issue	Result
✱	Windows Security Updates	6 security updates could not be confirmed. What was scanned Result details How to correct this
✓	Microsoft VM Security Updates	No critical security updates are missing. What was scanned
✓	Office Updates	No critical security updates are missing. What was scanned
✓	Windows Media Player Security Updates	No critical security updates are missing. What was scanned
✓	MDAC Security Updates	No critical security updates are missing. What was scanned
✓	MSXML Security Updates	No critical security updates are missing. What was scanned

Windows Scan Results

Vulnerabilities

The following pages show an exported version of the MBSA report for the baseline system. This report is annotated with the expected values for a production system to be in compliance with the baseline and comments on the significance of each item.

Computer name:	C840\C840BASELINE
IP address:	127.0.0.1
Security report name:	LAT800 - LAT800BASELINE (3-16-2005 3-18 PM)
Scan date:	3/16/2005 3:18 PM
Security update database version:	2005.2.25.0
Office update database version:	11.0.0.7503
Security assessment:	Potential Risk (One or more non-critical checks failed.)

Security Updates

Score	Issue	Expected Result / Impact
Check passed	MDAC Security Updates	No critical security updates are missing. KB870669 present in baseline
Check passed	Microsoft VM Security Updates	No critical security updates are missing.
Check passed	MSXML Security Updates	No critical security updates are missing. Baseline is Version 3.0, SP 5

Check passed	Office Updates	No critical security updates are missing.
Check passed	Windows Media Player Security Updates	No critical security updates are missing. KB885492, KB828026 present in baseline
Best practice	Windows Security Updates	6 security updates could not be confirmed: Q327522, Q814078, Q819696, 839643, Q833987, Q890261 This is a known problem with MBSA (REF: Microsoft Knowledge Base article Q306460) Confirm installation of these updates in Add/Remove Programs. All available updates were applied to the baseline system image: KB823182, KB823559, KB824105, KB825119, KB826232, KB828035, KB828741, KB828749, KB835732, KB837001, KB839645, KB840315, KB840987, KB841356, KB841533, KB841872, KB841873, KB842526, KB867282, KB871250, KB873333, KB873339, KB885250, KB885835, KB885836, KB888113, KB890047, KB890175, KB891711, KB891781 If any of the updates listed above are missing, this is an exception. If MBSA reports newer updates as missing, these should be considered for inclusion in the baseline. A missing update leaves the system vulnerable to exploitation.

Windows Scan Results

Vulnerabilities

Score	Issue	Expected Result

Check passed	Administrators	No more than 2 Administrators were found on this computer. **User** Minad and localadm are the designated administrator accounts for this baseline. Any additional members of the administrators group would constitute an exception. Unnecessary administrator access for users violates the principal of least privilege. Unexpected members of the administrators group may indicate a successful privilege escalation attack.
Check passed	Autologon	Autologon is not configured on this computer. Autologon causes the system to automatically log in a specified user account upon start up. This bypasses user authentication and generally lessens security. Valid uses for Autologon, such as in a 'kiosk computer', do not apply to this baseline.
Check Failed (non-critical)	Automatic Updates	Updates are not automatically downloaded or installed on this computer. Automatic update is suppresses so that updates are only installed after being approved by the organization. When the organization's Windows Update Server is operational, the baseline will include a configuration to download and install the approved updates from that server.

Check passed	File System	All hard drives (1) are using the NTFS file system. **Drive Letter** **File System** C: NTFS FAT and FAT32 volumes cannot be secured because they lack the access control, auditing and encryption features available in NTFS.
Check passed	Guest Account	The Guest account is disabled on this computer. The guest account allows effectively anonymous users to have access to the system and should always be disabled.
Check passed	Local Account Password Test	No user accounts have blank or simple passwords. Our security template mandates complex passwords of at least eight characters. A blank or simple password could indicate an intrusion or poor system administration.
Check failed (non-critical)	Password Expiration	Some user accounts (2 of 3) have non-expiring passwords. **User** Guest - permanently disabled Minad - built-in local administrator account

Check passed	Restrict Anonymous	RestrictAnonymous = 2. This prevents 'null session' network access to the system.
Best practice	Windows Firewall	Windows Firewall is not installed or configured properly, or is not available on this version of Windows. Symantec Client Firewall is installed.

Additional System Information

Score	Issue	Expected Result
Best practice	Auditing	Logon Success and Logon Failure auditing are both enabled. Our template specifies an even higher level of auditing. However, auditing logon events is essential to detecting who has accessed the system and to detecting password guessing attacks.
Best practice	Services	Some potentially unnecessary services are installed. **Service** **State** Telnet Stopped Telnet is disabled by the security template . MBSA should not report any other problem services.

Additional information	Shares	No shares are present on your computer. The baseline security template disables the default administrative shares. Given the stand alone nature of this system, the default administrative shares do not add value and present a point of vulnerability.
Additional information	Windows Version	Computer is running Windows 2000 or greater.

Internet Information Services (IIS) Scan Results

Score	Issue	Expected Result
Check not performed	IIS Status	IIS is not running on this computer. This system does not need to provide web services or newsgroups.

SQL Server Scan Results

Score	Issue	Expected Result
Check not performed	SQL Server/MSDE Status	SQL Server and/or MSDE is not installed on this computer. This system does not require a database.

Desktop Application Scan Results

Vulnerabilities

Score	Issue	Expected Result
Check passed	IE Zones	Internet Explorer zones have secure settings for all users. Low zone settings leave the system vulnerable to several attacks through malicious web pages and other sources.

Check passed	Macro Security	4 Microsoft Office product(s) are installed. No issues were found. Macro security is set to high for all users. **Issue** **User** **Advice** Microsoft Excel 2000 All Users No security issues were found. Microsoft Outlook 2000 All Users No security issues were found. Microsoft PowerPoint 2000 All Users No security issues were found. Microsoft Word 2000 All Users No security issues were found. Macro security should be set to 'high' for all users on all these applications. Embedded macros in Office documents can be malicious code and could execute automatically at a lower setting.

Antivirus and Client Firewall Software.

We need to ensure that the antivirus software and client firewall on the system are installed and operating properly.

If any of this software is disabled or has its configuration altered, it will leave the system vulnerable. This is also often an indication of an intrusion or the presence of malicious software, since disabling these applications reduces the chance of detection and allows easier access to the system.

Item	Baseline Setting

Start up	Symantec Client Security runs on start up. We need to ensure the system is protected at all times.
File System Auto-protect	Enabled for all file types. We need the antivirus software to protect the system in real-time and examine all file types.
Internet E-mail Auto-protect	Enabled for all file types. We want the AV software to examine all email attachments. This is a significant vector for malicious software to propagate.
Microsoft Exchange Auto-protect	Enabled for all file types. We want the AV software to examine all email attachments. This is a significant vector for malicious software to propagate.
Update Schedule (Live Update)	Daily updates We want to have the latest threat signatures on the system. The signatures are often updated multiple times in a single week.
Scheduled Scans	Weekly full system scan. We wish to periodically examine the whole system to look for threats. However, scanning too frequently can bog the system down and lead users to attempt to disable the software.
Client Firewall Configuration	Turned on and set to 'high'. We wish to have the maximum level of protection from network threats. The approved set of software in the baseline will not be impeded by the 'high' setting.
Client Firewall Configuration	No entries in the Trusted Zone We have no requirement to allow any IP address to bypass the firewall.
Intrusion Detection Configuration	Turned on with AutoBlock turned on. We wish to detect threats attempting to enter or leave the system. AutoBlock helps to avoid the effect of port scans, brute force attacks and denial of service traffic on the system.
Privacy Control	Turned on, medium level. We wish to protect privacy on the system. The high setting is too restrictive, blocking all browser cookies and generating many alerts.

2.6 Inventory of Installed Software.

An inventory of the installed software is part of the baseline. Knowing what software to expect on a system is a critical part of making it secure. We cannot secure it if we do not know it is there. Combined with the file system mapping detailed in 2.2, this gives us thorough knowledge of what is on our system. Having an efficient method of collecting a software inventory makes it relatively easy to evaluate production systems against the baseline.

We use the Microsoft Application Compatibility Analyzer (MACA) to collect this data. This software package was originally intended to provide application compatibility information in support of operating system upgrades. However, the package also works well as a software inventory tool for windows-based systems. This package can quickly scan a system and return a list of the installed software. The collector portion of this package can scan multiple systems on a network as well as stand-alone systems. We will detail the technique for collecting a software inventory from a stand-alone system. A discussion of using Microsoft Compatibility Analyzer as a software inventory system is given in [Liang04].

The Microsoft Application Compatibility Analyzer report provides an easy, human-readable means to determine if the installed software has changed from the baseline. This report works hand-in-hand with the FTimes comparison report to identify changes. File differences reported by FTimes might be readily explained in the MACA report, possibly by the presence (or absence) of software or by the changes in a version of baseline software. This goes a long way towards determining the significance of changes detected with FTimes.

Software Inventory Procedure.

We have downloaded the Microsoft Application Compatibility Analyzer and installed in on a trusted workstation. This product is available as a no-cost download from Microsoft. [http://www.microsoft.com/downloads/details.aspx?FamilyID=7fc46855-b8a4-46cd-a236-3159970fde94&DisplayLang=en]

The trusted workstation holds the software inventory report from the baseline image and reports collected from other systems to assess their compliance with the baseline.

We use the Collector portion of the Microsoft Application Compatibility Analyzer package (Collector.exe) to inventory the applications installed on the system. The Collector application does not need to be installed on the target system. It can collect this information across a network; however, for this procedure we are using a removable USB drive to maintain an 'air gap' between this system and our network.

1) Insert the USB drive into the USB port on the C840. It will mount as drive E:

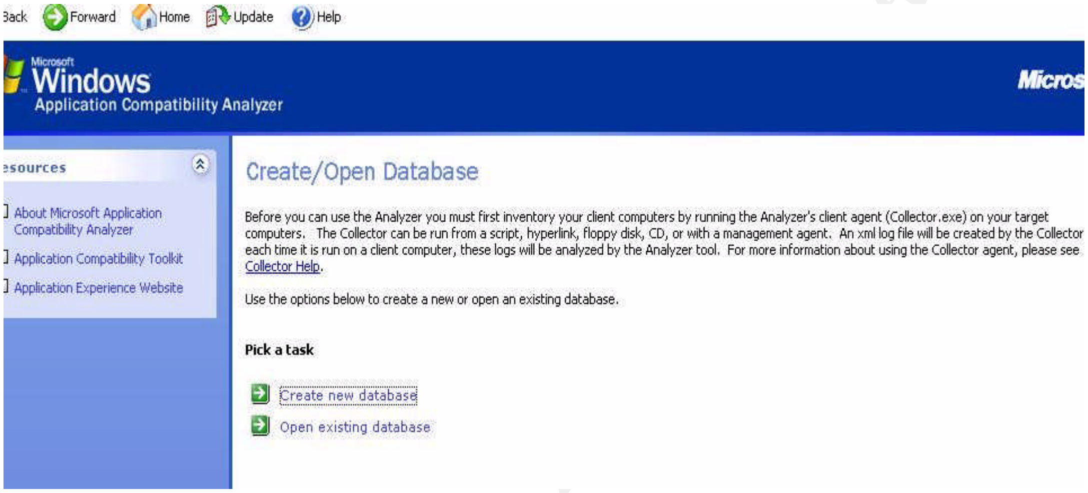
2) Open the command prompt and enter: "C:>E:\collector.exe /O E:/" Collector.exe will scan the entire system. An icon will appear in the system tray during the scan. Collector.exe will write the output file to the USB drive (E:).

3) Stop the USB drive and remove it from the system. Connect the USB drive to the trusted workstation with the MACA.

4) Launch the Microsoft Application Compatibility Analyzer.

-Click 'Start using the analyzer'.

-Click 'Create a new database.'


Back
Forward
Home
Update
Help
Microsoft Windows
Application Compatibility Analyzer
Micros
esources
About Microsoft Application Compatibility Analyzer
Application Compatibility Toolkit
Application Experience Website

Create/Open Database

Before you can use the Analyzer you must first inventory your client computers by running the Analyzer's client agent (Collector.exe) on your target computers. The Collector can be run from a script, hyperlink, floppy disk, CD, or with a management agent. An xml log file will be created by the Collector each time it is run on a client computer, these logs will be analyzed by the Analyzer tool. For more information about using the Collector agent, please see Collector Help.

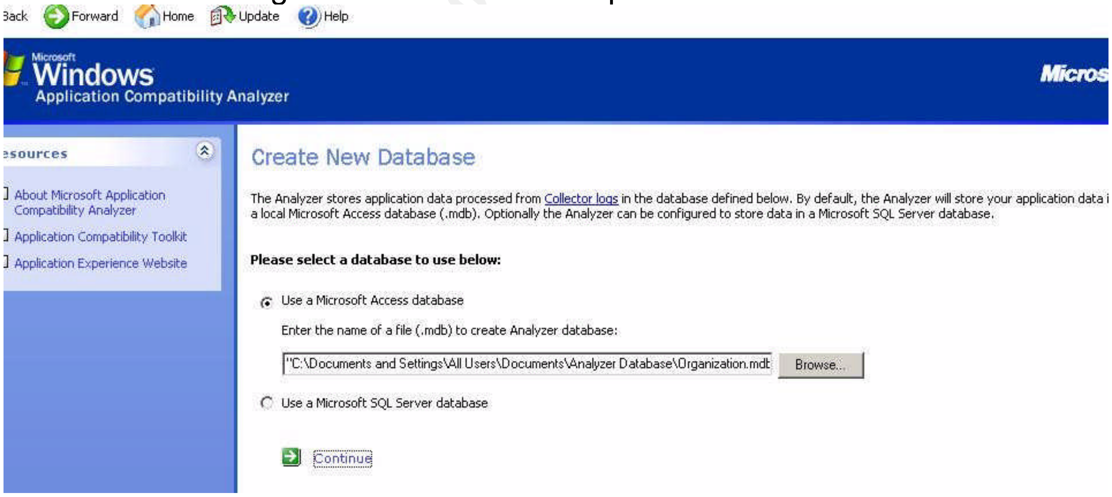
Use the options below to create a new or open an existing database.

Pick a task

Create new database

Open existing database

-Select the 'Use a Microsoft Access Database' radio button. The default database name 'organization.mdb' is acceptable.


Back
Forward
Home
Update
Help
Microsoft Windows
Application Compatibility Analyzer
Micros
esources
About Microsoft Application Compatibility Analyzer
Application Compatibility Toolkit
Application Experience Website

Create New Database

The Analyzer stores application data processed from Collector logs in the database defined below. By default, the Analyzer will store your application data i a local Microsoft Access database (.mdb). Optionally the Analyzer can be configured to store data in a Microsoft SQL Server database.

Please select a database to use below:

● Use a Microsoft Access database

Enter the name of a file (.mdb) to create Analyzer database:

"C:\Documents and Settings\All Users\Documents\Analyzer Database\Organization.mdb Browse...

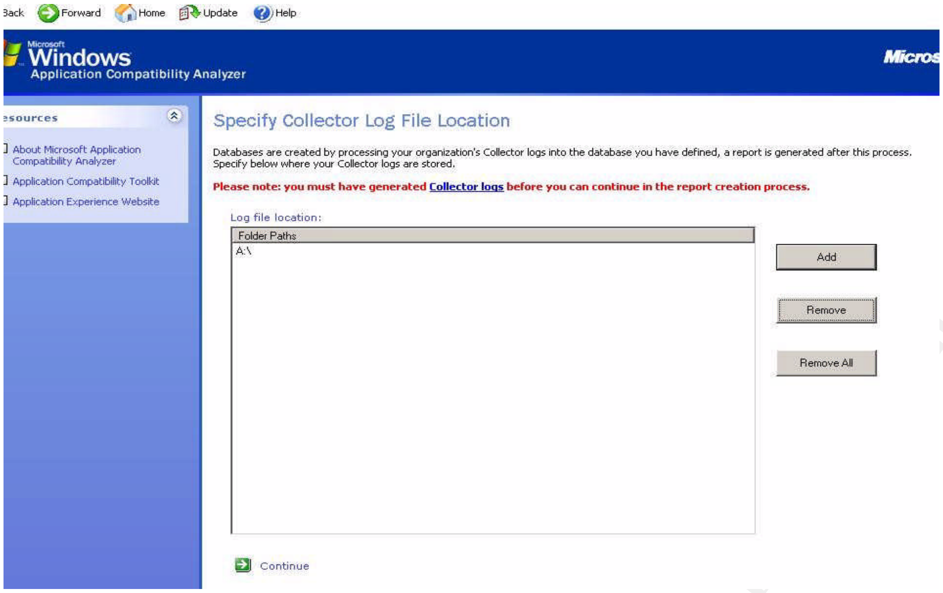
○ Use a Microsoft SQL Server database

Continue

-Click Continue

-On the 'Specify Collector Log File Location' page, if the path to the USB drive is not shown, click the Add button. Browse to find the USB drive and click OK.

-Click Continue.


Back
Forward
Home
Update
Help
Microsoft Windows Application Compatibility Analyzer
Micros
esources
About Microsoft Application Compatibility Analyzer
Application Compatibility Toolkit
Application Experience Website
Add
Remove
Remove All
Continue

Specify Collector Log File Location

Databases are created by processing your organization's Collector logs into the database you have defined, a report is generated after this process. Specify below where your Collector logs are stored.

Please note: you must have generated Collector logs before you can continue in the report creation process.

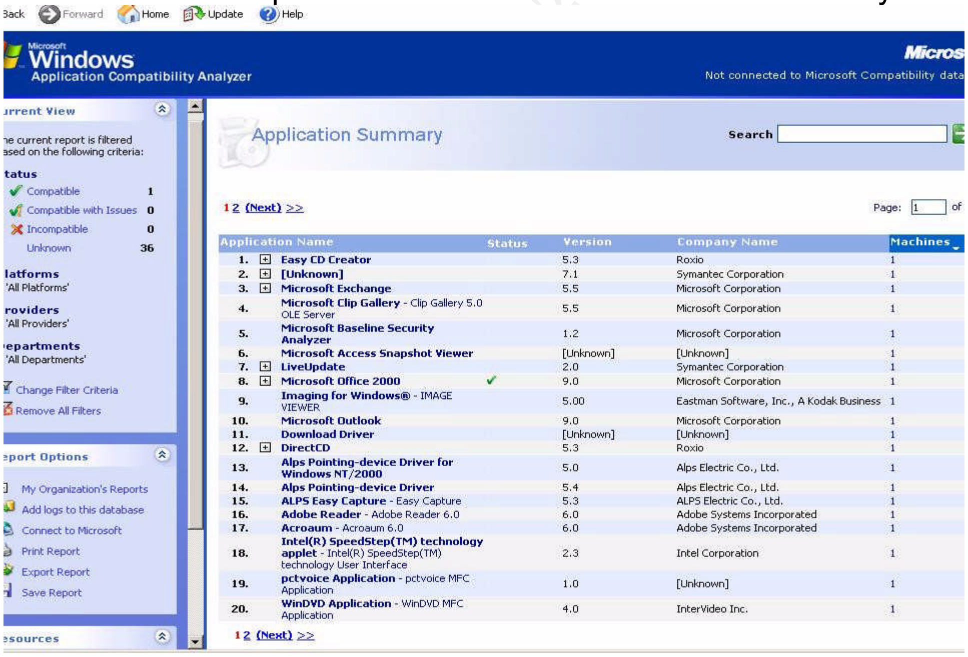
Log file location:

Folder Paths
A:\

-When prompted: "Connect to the Compatibility Database at Microsoft" click the No radio button and then click Continue. This information is not needed for a simple software inventory.

-The collector log file will be read from the USB drive. Click the 'Start' button on the page to add this information to the database.

-View the report. This is our baseline software inventory.



he current report is filtered ased on the following criteria:

tatus

✓ Compatible	1
✓ Compatible with Issues	0
✗ Incompatible	0
Unknown	36

latforms
'All Platforms'

roviders
'All Providers'

epartments
'All Departments'

Application Summary

Application Name			Status	Version	Company Name	Machines
1.	⊞	**Easy CD Creator**		5.3	Roxio	1
2.	⊞	**[Unknown]**		7.1	Symantec Corporation	1
3.	⊞	**Microsoft Exchange**		5.5	Microsoft Corporation	1
4.		**Microsoft Clip Gallery** - Clip Gallery 5.0 OLE Server		5.5	Microsoft Corporation	1
5.		**Microsoft Baseline Security Analyzer**		1.2	Microsoft Corporation	1
6.		**Microsoft Access Snapshot Viewer**		[Unknown]	[Unknown]	1
7.	⊞	**LiveUpdate**		2.0	Symantec Corporation	1
8.	⊞	**Microsoft Office 2000**	✓	9.0	Microsoft Corporation	1
9.		**Imaging for Windows®** - IMAGE VIEWER		5.00	Eastman Software, Inc., A Kodak Business	1
10.		**Microsoft Outlook**		9.0	Microsoft Corporation	1
11.		**Download Driver**		[Unknown]	[Unknown]	1
12.	⊞	**DirectCD**		5.3	Roxio	1
13.		**Alps Pointing-device Driver for Windows NT/2000**		5.0	Alps Electric Co., Ltd.	1
14.		**Alps Pointing-device Driver**		5.4	Alps Electric Co., Ltd.	1
15.		**ALPS Easy Capture** - Easy Capture		5.3	ALPS Electric Co., Ltd.	1
16.		**Adobe Reader** - Adobe Reader 6.0		6.0	Adobe Systems Incorporated	1
17.		**Acroaum** - Acroaum 6.0		6.0	Adobe Systems Incorporated	1
18.		**Intel(R) SpeedStep(TM) technology applet** - Intel(R) SpeedStep(TM) technology User Interface		2.3	Intel Corporation	1
19.		**pctvoice Application** - pctvoice MFC Application		1.0	[Unknown]	1
20.		**WinDVD Application** - WinDVD MFC Application		4.0	InterVideo Inc.	1

This report is stored on the trusted workstation. It can also be exported to a comma separated values file and imported into another application, such as a spread sheet, for formatting or analysis.

SUITE_NAME	MACHINE_COUNT	SIGNATURE	APPLICATION_NAME	COMPANY_NAME	VERSION	EXE_NAME	LANGUAGE	MODULE_TYPE
[Unknown]	2	-1629685139	Log Exporter	Symantec Corporation	7.1.0.577	LOGEXPRT.EXE	English (United States) [0x409]	32 bit
[Unknown]	2	-1027841506	Program Scanner	Symantec Corporation	7.1.0.577	ALESCAN.EXE	English (United States) [0x409]	32 bit
[Unknown]	2	2087958097	Statistics	Symantec Corporation	7.1.0.577	IAMSTATS.EXE	English (United States) [0x409]	32 bit
Acroaum	2	912425045	Acroaum 6.0	Adobe Systems Incorporated	6.0.0.0	ACROAUM.EXE	English (United States) [0x409]	32 bit
Adobe Reader	2	-384377972	Adobe Reader 6.0	Adobe Systems Incorporated	6.0.1.2003110300	ACRORD32.EXE	English (United States) [0x409]	32 bit
ALPS Easy Capture	2	-841670310	Easy Capture	ALPS Electric Co., Ltd.	5.3.1.39	Ezcapt.exe	Japanese [0x411]	32 bit
Alps Pointing-device Driver	2	1449277737	Alps Pointing-device Driver	Alps Electric Co., Ltd.	5.4.101.113	Apoint.exe	Japanese [0x411]	32 bit
Alps Pointing-device Driver for	2	-373494743	Alps Pointing-device Driver for	Alps Electric Co., Ltd.	5.0.1.13	ApntEx.exe	Japanese [0x411]	32 bit
DirectCD	2	1959099913	DirectCD Application	Roxio	5.3.4.21	DIRECTCD.EXE	English (United States) [0x409]	32 bit
DirectCD	2	2080247399	EasyWrite Reader Installer	Roxio	5.3.4.21	MRFINST.EXE	English (United States) [0x409]	32 bit
Download Driver	2	977527542	Download Driver			CONSOLEAPP.EXE		32 bit
Easy CD Creator	2	-1967339759	Roxio CD Copier	Roxio	5.3.4.21	CDCOPIER.EXE	English (United States) [0x409]	32 bit
Easy CD Creator	2	44173917	Roxio Create CD	Roxio	5.3.4.21	CREATECD50.EXE	English (United States) [0x409]	32 bit
Easy CD Creator	2	-2062371019	Roxio EasyCDCreator	Roxio	5.3.4.21	CREATR50.EXE	English (United States) [0x409]	32 bit
Imaging for Windows®	2	543418592	IMAGE VIEWER	Eastman Software, Inc., A Kodak Business	5.00.2138.1	KODAKIMG.EXE	English (United States) [0x409]	32 bit
Intel(R) SpeedStep(TM)	2	-623678414	Intel(R) SpeedStep(TM)	Intel Corporation	2.3.0.0	PRPCUI.EXE	English (United States) [0x409]	32 bit
LiveUpdate	2	2127762557	Automatic LiveUpdate Module	Symantec Corporation	2.0.39.0	AUPDATE.EXE	English (United States) [0x409]	32 bit
LiveUpdate	2	-1023625934	LiveUpdate Engine COM	Symantec Corporation	2.0.39.0	LUCOMSERVER.EXE	English (United States) [0x409]	32 bit
LiveUpdate	2	596241197	LiveUpdate Wizard	Symantec Corporation	2.0.39.0	LUALL.EXE	English (United States) [0x409]	32 bit
LiveUpdate	2	-1331781793	Symantec ALUNotify Module	Symantec Corporation	2.0.39.0	ALUNOTIFY.EXE	English (United States) [0x409]	32 bit
LiveUpdate	2	1920985424	Symantec LUInit Module	Symantec Corporation	2.0.39.0	LUINIT.EXE	English (United States) [0x409]	32 bit
LiveUpdate	2	-2050186408	Symantec NetDetect	Symantec Corporation	2.0.39.0	NDETECT.EXE	English (United States) [0x409]	32 bit
Microsoft Access Snapshot	2	-1355539272	Microsoft Access Snapshot			MISC.EXE		32 bit
Microsoft Baseline Security	2	691679327	Microsoft Baseline Security	Microsoft Corporation	1.2.1	MBSA.EXE	English (United States) [0x409]	32 bit
Microsoft Clip Gallery	2	1837526835	Clip Gallery 5.0 OLE Server	Microsoft Corporation	5.5.01.0522	ARTGALRY.EXE	English (United States) [0x409]	32 bit
Microsoft Exchange	2	-349545878	Extended MAPI 1.0 for	Microsoft Corporation	5.5	MAPISRVR.EXE	English (United States) [0x409]	32 bit
Microsoft Exchange	2	-1924008648	Microsoft Exchange	Microsoft Corporation	5.5	OUT40.EXE	English (United States) [0x409]	32 bit
Microsoft Exchange	2	2018259444	Microsoft Outlook Profile	Microsoft Corporation	5.5	NEWPROF.EXE	English (United States) [0x409]	32 bit
Microsoft Exchange	2	883689018	Outlook Conflict Note	Microsoft Corporation	8.2	CNFNOT32.EXE	English (United States) [0x409]	32 bit
Microsoft Office 2000	2	20973031	Microsoft Excel for Windows	Microsoft Corporation	9.0.8924	EXCEL.EXE	Language Neutral [0x0]	32 bit
Microsoft Office 2000	2	840650106	Microsoft Office 2000	Microsoft Corporation	9.0.3720	OSA9.EXE	Language Neutral [0x0]	32 bit
Microsoft Office 2000	2	1026487739	Microsoft Office 2000	Microsoft Corporation	9.0.2702	BINDER.EXE	Language Neutral [0x0]	32 bit
Microsoft Office 2000	2	-1837576034	Microsoft Office 2000	Microsoft Corporation	9.0.3502	MSOHELP.EXE	English (United States) [0x409]	32 bit
Microsoft Office 2000	2	-323096974	Microsoft Word for Windows	Microsoft Corporation	9.0.8216	WINWORD.EXE	Language Neutral [0x0]	32 bit
Microsoft Outlook	2	-139223891	Microsoft Outlook	Microsoft Corporation	9.0.6604	OUTLOOK.EXE	Language Neutral [0x0]	32 bit
Microsoft Photo Editor	2	-1478705321	Microsoft Photo Editor	Microsoft Corporation	3.01.3	PHOTOED.EXE	English (United States) [0x409]	32 bit
Microsoft PowerPoint for	2	-831350472	Microsoft PowerPoint for	Microsoft Corporation	9.0.6620	POWERPNT.EXE	Language Neutral [0x0]	32 bit
Microsoft Synchronization	2	-1598374517	Microsoft Synchronization	Microsoft Corporation	5.00.2195.6627	MOBSYNC.EXE	English (United States) [0x409]	32 bit
Microsoft(R) Windows Media	2	1805865728	Windows Media Player	Microsoft Corporation	9.00.00.2980	WMPLAYER.EXE	English (United States) [0x409]	32 bit
Microsoft® Access	2	-1238752445	Microsoft Access for Windows	Microsoft Corporation	9.0.6620	MSACCESS.EXE	Language Neutral [0x0]	32 bit
Microsoft® Reader	1	-197287793	Microsoft Reader	Microsoft Corporation	Version 2.1.1	msreader.exe	English (United States) [0x409]	32 bit
Norton AntiSpam	2	917596038	AD Trash Can	Symantec Corporation	2004.2	ADTRASH.EXE	English (United States) [0x409]	32 bit
NVIDIA nView Wizard, Version	2	-378621156	NVIDIA nView Wizard, Version	NVIDIA Corporation	6.13.10.4258	NWIZ.EXE	English (United States) [0x409]	32 bit
pctvoice Application	2	1814796558	pctvoice MFC Application		1, 0, 0, 1	PCTSPK.EXE	English (United States) [0x409]	32 bit
Projector Wizard	2	-1324560112	Projector Wizard	In Focus Systems, Inc.	1	PROJWIZ.EXE	English (United States) [0x409]	32 bit
Roxio Migration Wizard	2	2035783944	Roxio Migration Wizard	Roxio	5.3.0.0	MIGRATE.EXE	English (United States) [0x409]	32 bit
Symantec AntiVirus	2	-1001811474	Symantec AntiVirus	Symantec Corporation	9.0.0.338	RTVSCAN.EXE	English (United States) [0x409]	32 bit
Symantec AntiVirus	2	-96178182	Symantec AntiVirus	Symantec Corporation	9.0.0.338	VPC32.EXE	English (United States) [0x409]	32 bit
Symantec AntiVirus	2	-968281790	Virus Definition Daemon	Symantec Corporation	9.0.0.338	DEFWATCH.EXE	English (United States) [0x409]	32 bit
Symantec Client Firewall	2	-995542703	Alert Assistant	Symantec Corporation	7.1	ALERTAST.EXE	English (United States) [0x409]	32 bit
Symantec Client Firewall	2	-1114991786	Configuration Wizard Service	Symantec Corporation	7.1	CFGWZSVC.EXE	English (United States) [0x409]	32 bit
Symantec Client Firewall	2	765746511	FIO	Symantec Corporation	7.1	FIO.EXE	English (United States) [0x409]	32 bit
Symantec Client Firewall	2	-1122725487	Home Network Wizard	Symantec Corporation	7.1	HNETWIZ.EXE	English (United States) [0x409]	32 bit
Symantec Client Firewall	2	-239992190	NIS Email Server	Symantec Corporation	7.1	NISEMSVR.EXE	English (United States) [0x409]	32 bit
Symantec Client Firewall	2	-2134458613	NisMediator	Symantec Corporation	7.1	NSMDTR.EXE	English (United States) [0x409]	32 bit
Symantec Client Firewall	2	604191687	SymSPort.exe	Symantec Corporation	7.1	SYMSPORT.EXE	English (United States) [0x409]	32 bit
Symantec Integrator	2	-1232360498	Symantec Integrator	Symantec Corporation	6.7.0.577	NMAIN.EXE	English (United States) [0x409]	32 bit
Symantec SAVRoam	2	626959924	SAVRoam	symantec	1.5.0.0	SAVROAM.EXE	English (United States) [0x409]	32 bit
Symantec Security Drivers	2	1312684738	IDS Core Updater	Symantec Corporation	5.3.5	IDSCOLU.EXE	English (United States) [0x409]	32 bit
Symantec Security Drivers	2	-754464182	IDS Updater	Symantec Corporation	5.3	IDSLU.EXE	English (United States) [0x409]	32 bit
WinDVD Application	2	-1448343638	WinDVD MFC Application	InterVideo Inc.	4	WINDVD.EXE	English (United States) [0x409]	32 bit
WinZip	2	-652462326	WinZip Executable	WinZip Computing, Inc.	8.0 (3105)	WINZIP32.EXE	English (United States) [0x409]	32 bit

2.7 Summary.

At the conclusion of this process we have a good picture of what 'right' looks like on our system. The baseline includes deliverables detailing the state of the operating system and the installed software. It also includes the configuration settings needed to make the system secure. These items overlap somewhat in their scope, but this makes it easier to detect and analyze deviations from the baseline. In addition, the tools and techniques used also have the advantage of being publicly available at no cost.

SECTION 3 : TESTING AGAINST THE BASELINE

3.1 Overview.

The procedures for testing a production system against the baseline are very similar to the procedures for taking the baseline itself:

1) Take snapshot map of the file system and compare it to the baseline map to detect changes.

2) Compare the current security configuration on the system against the baseline settings in the organizational security template.

3) Compare the other, non-template, security settings with the expected baseline results.

4) Take an inventory of the installed software and compare with the baseline software inventory.

The result of these procedures will allow us to determine if the system is in compliance with the baseline, what potential security issues might be present, and most importantly, whether or not the system can still be considered secure.

3.2. Compare A Snapshot File System Map With The Baseline File System Map.

We will again use FTimes to map the file system. This time we will compare the snapshot map with the baseline map to find any difference.

Procedure.

1) Ensure a valid copy of the baseline map file is on the USB drive. In this case it will be called 'C840BL.map'.

2) Boot the system using the Knoppix STD CD:
-Power the system on and press F12 for the boot menu.
-Insert the CD into the drive and select it as the boot device
-At the boot prompt, enter 'fb1024x768' to get a readable display

3) Mount the drives:
-Right click on the desktop
-Select 'Forensics' from the context menu and then 'Forensics Shell' from the forensics menu.
-Mount the NTFS volume read-only. At the forensics shell command line:

```
root@1[forensics]# mount -r -t ntfs  /dev/hda1 /mnt/hda1
```

-Insert the USB drive into the USB port and mount it as a MS DOS volume:

```
root@1[forensics]# mount -t msdos /dev/sda1 /mnt/sda1
```

4) Take the file system snapshot with FTimes using snapshot.cfg

```
root@1[forensics]# ftimes --mapfull /mnt/sda1/snapshot.cfg
```

The contents of snapshot.cfg:

```
BaseName=C840
OutDir=/mnt/sda1/
RunType=snapshot
FieldMask=NONE+mtime+size+md5
Include=/mnt/hda1
Exclude=/mnt/hda1/Documents and Settings
```

The only difference from baseline configuration file in 2.3 above is that the RunType is 'snapshot' rather than 'baseline'.

This will write a copy of the snapshot map file onto the USB drive. In this case, it saves to a file named 'C840_200.map'

5) Compare baseline map with snapshot map, redirecting output to USB drive.

The format for this FTimes function is:

```
ftimes --compare <filemask> <baseline> <shapshot>
```

The output defaults to stdout. We will redirect it to a file on the USB drive so we can more easily analyze the results. Thus, the final command is:

```
root@1[forensics]# ftimes --compare NONE+mtime+size+md5
/mnt/sda1/C840BL.map /mnt/sda1/C840_200.map > /mnt/sda1/compar1.txt
```

This writes the results of the comparison to the file 'compar1.txt' on the USB drive.

6) Now we can examine the results in the comparison file.

We are most interested in changes to executable files in the file system. New or modified executable files can represent a compromise of the system or simply new software added. A list of typical Windows 2000 executable file types is below: [Vibert00]

.ACM	Audio Compression Module add-on	Windows System file
.CMD	Windows NT batch file	Windows 32-bit Exec.
.CPL	Control Panel extension	Windows 16-bit Exec.
.DEV	Device driver	Windows 32-bit Exec.
.DLL	Dynamic Link Library	Windows 16-bit Exec.
.DL? (.DLL)	Dynamic Link Library	Windows 32-bit Exec.
.DRV	Device driver	Windows 32-bit Exec.
.EXE	DIET, PKLITE, LZEXE, UPX, etc.	Compressed exec. files
.EXE	New Executable	Windows 16-bit Exec.
.EXE	Portable Executable	Windows 32-bit Exec.
.HLP	Help files	Windows 16-bit Exec.
.LNK	Shortcut file	Windows Executable
.MOD	Kernel Module	Windows 16-bit Exec.
.MSC	Microsoft Common Console Doc	
.MSI	MS Windows Installer File	File archives
.MSP	Windows Installer Patch	
.PCI	Windows PCI Miniport system file	Windows Exec.
.PIF	Program Information File	Windows Exec.
.REG	Windows Registry files	
.SCR	Screen saver	Windows 16-bit Exec.
.SYS	Win NT device driver	Windows 32-bit Exec.
.TSP	Windows Telephony Service	Windows Exec.
.VXD	Virtual Device Drivers	Windows 32-bit Exec.
.VWP	Audio plug-in	Windows Exec.
.WIN	Window file	Windows 32-bit Exec.
.??	MS Compress/Expand	Compressed exec. files
.286	Device driver for Windows 2.0 and 3.x real mode	
.386	Virtual device driver	Windows 16-bit Exec.

Some files and file types will routinely change during system operation and do not normally pose a security risk. We would expect these files to show up as changed each time we compared a snapshot to the baseline.

pagefile.sys	The virtual memory page file
.tmp	Temporary files
.log	Log files
.evt	Windows event log files
.dat	Data files. The installed Symantec products change their .dat files during operation.
.SAM	The Windows Security Accounts Manager file
.bak	Backup files

It is generally safe to ignore changes to these types of files, but if in doubt, investigate.

Now we can take a look at a sample comparison report. The FTimes comparison report has the following fields:

Category - indicates if the difference is a change from the baseline, C, or a new file, N.

Name - the file name. The path is derived from the Linux mount point we used, so '/mnt/hda1' is equivalent to 'C:\' in Windows 2000.

Changed - indicated which fields have changed. In this baseline we are monitoring the last time of modification (*mtime*), the size of the file (*size*) and the file's MD5 value (*md5*).

compar1.txt

```
category|name|changed|
C|"/mnt/hda1/pagefile.sys"|mtime,md5|
C|"/mnt/hda1/Program+Files/Common+Files/Adaptec+Shared/CreateCD/Images/ButtonCoords.in
i"|mtime|
C|"/mnt/hda1/Program+Files/Common+Files/InstallShield/engine/6/Intel+32"|mtime|
N|"/mnt/hda1/Program+Files/Common+Files/Microsoft+Shared/ClearType/ctras-dll.sig"||
N|"/mnt/hda1/Program+Files/Common+Files/Microsoft+Shared/ClearType/ctras.dll"||
N|"/mnt/hda1/Program+Files/Common+Files/Microsoft+Shared/ClearType"||
C|"/mnt/hda1/Program+Files/Common+Files/Microsoft+Shared"|mtime|
C|"/mnt/hda1/Program+Files/Common+Files/Symantec+Shared/profile.dat"|mtime|
C|"/mnt/hda1/Program+Files/Common+Files/Symantec+Shared/SNDALRT.log"|mtime|
C|"/mnt/hda1/Program+Files/Common+Files/Symantec+Shared/SNDCON.log"|mtime|
C|"/mnt/hda1/Program+Files/Common+Files/Symantec+Shared/SNDDBG.log"|mtime|
C|"/mnt/hda1/Program+Files/Common+Files/Symantec+Shared/SNDFW.log"|mtime,size,md5|
C|"/mnt/hda1/Program+Files/Common+Files/Symantec+Shared/SNDIDS.log"|mtime,size,md5|
C|"/mnt/hda1/Program+Files/Common+Files/Symantec+Shared/SNDSYS.log"|mtime,size,md5|
C|"/mnt/hda1/Program+Files/Common+Files/Symantec+Shared/Validate.dat"|mtime,md5|
N|"/mnt/hda1/Program+Files/InstallShield+Installation+Information/{B6F7DBE7-2FE2-458F-A738-
B10832746036}/data1.cab"||
N|"/mnt/hda1/Program+Files/InstallShield+Installation+Information/{B6F7DBE7-2FE2-458F-A738-
B10832746036}/data1.hdr"||
N|"/mnt/hda1/Program+Files/InstallShield+Installation+Information/{B6F7DBE7-2FE2-458F-A738-
B10832746036}/layout.bin"||
N|"/mnt/hda1/Program+Files/InstallShield+Installation+Information/{B6F7DBE7-2FE2-458F-A738-
B10832746036}/Setup.exe"||
N|"/mnt/hda1/Program+Files/InstallShield+Installation+Information/{B6F7DBE7-2FE2-458F-A738-
B10832746036}/setup.ilg"||
N|"/mnt/hda1/Program+Files/InstallShield+Installation+Information/{B6F7DBE7-2FE2-458F-A738-
B10832746036}/Setup.ini"||
N|"/mnt/hda1/Program+Files/InstallShield+Installation+Information/{B6F7DBE7-2FE2-458F-A738-
B10832746036}/setup.inx"||
N|"/mnt/hda1/Program+Files/InstallShield+Installation+Information/{B6F7DBE7-2FE2-458F-A738-
B10832746036}"||
C|"/mnt/hda1/Program+Files/InstallShield+Installation+Information"|mtime|
N|"/mnt/hda1/Program+Files/Microsoft+Reader/aud_file.dll"||
N|"/mnt/hda1/Program+Files/Microsoft+Reader/dmgr-dll.sig"||
N|"/mnt/hda1/Program+Files/Microsoft+Reader/dmgr.dll"||
N|"/mnt/hda1/Program+Files/Microsoft+Reader/d_Aud1.dll"||
N|"/mnt/hda1/Program+Files/Microsoft+Reader/ebookfx-dll.sig"||
N|"/mnt/hda1/Program+Files/Microsoft+Reader/EBOOKFX.dll"||
N|"/mnt/hda1/Program+Files/Microsoft+Reader/ebriched-dll.sig"||
N|"/mnt/hda1/Program+Files/Microsoft+Reader/ebriched.dll"||
N|"/mnt/hda1/Program+Files/Microsoft+Reader/eula.txt"||
N|"/mnt/hda1/Program+Files/Microsoft+Reader/guidebook.lit"||
N|"/mnt/hda1/Program+Files/Microsoft+Reader/imgdecmp.dll"||
N|"/mnt/hda1/Program+Files/Microsoft+Reader/msls31-dll.sig"||
N|"/mnt/hda1/Program+Files/Microsoft+Reader/msls31.dll"||
N|"/mnt/hda1/Program+Files/Microsoft+Reader/msreader-exe-manifest.sig"||
N|"/mnt/hda1/Program+Files/Microsoft+Reader/msreader-exe.sig"||
N|"/mnt/hda1/Program+Files/Microsoft+Reader/msreader.exe"||
N|"/mnt/hda1/Program+Files/Microsoft+Reader/oemeula.rtf"||
N|"/mnt/hda1/Program+Files/Microsoft+Reader/pid.txt"||
N|"/mnt/hda1/Program+Files/Microsoft+Reader/player_dll.dll"||
N|"/mnt/hda1/Program+Files/Microsoft+Reader/pts/pts.dat"||
N|"/mnt/hda1/Program+Files/Microsoft+Reader/pts"||
N|"/mnt/hda1/Program+Files/Microsoft+Reader/utils.dll"||
N|"/mnt/hda1/Program+Files/Microsoft+Reader"||
C|"/mnt/hda1/Program+Files/Symantec/LiveUpdate/ludirloc.dat"|mtime|
C|"/mnt/hda1/Program+Files/Symantec+Client+Security/Symantec+AntiVirus/savrt.dat"|mtime,md
5|
C|"/mnt/hda1/Program+Files/Symantec+Client+Security/Symantec+AntiVirus/SRTSEXCL.DAT"|m
time|
C|"/mnt/hda1/Program+Files/Symantec+Client+Security/Symantec+AntiVirus"|mtime|
C|"/mnt/hda1/Program+Files"|mtime|
C|"/mnt/hda1/WINNT/Tasks/SA.DAT"|mtime|
C|"/mnt/hda1/WINNT/system32/config/AppEvent.Evt"|mtime,md5|
C|"/mnt/hda1/WINNT/system32/config/default"|mtime,md5|
C|"/mnt/hda1/WINNT/system32/config/default.LOG"|mtime,md5|
C|"/mnt/hda1/WINNT/system32/config/SAM"|mtime,md5|
C|"/mnt/hda1/WINNT/system32/config/SAM.LOG"|mtime,md5|
C|"/mnt/hda1/WINNT/system32/config/SecEvent.Evt"|mtime,md5|
C|"/mnt/hda1/WINNT/system32/config/SECURITY"|mtime,md5|
C|"/mnt/hda1/WINNT/system32/config/SECURITY.LOG"|mtime,md5|
C|"/mnt/hda1/WINNT/system32/config/software"|mtime,md5|
C|"/mnt/hda1/WINNT/system32/config/software.LOG"|mtime,md5|
C|"/mnt/hda1/WINNT/system32/config/SysEvent.Evt"|mtime,md5|
C|"/mnt/hda1/WINNT/system32/config/system"|mtime,md5|
C|"/mnt/hda1/WINNT/system32/config/SYSTEM.ALT"|mtime,md5|
C|"/mnt/hda1/WINNT/system32/NtmsData/NTMSDATA"|mtime,md5|
C|"/mnt/hda1/WINNT/system32/NtmsData/NTMSDATA.BAK"|mtime,md5|
C|"/mnt/hda1/WINNT/system32/NtmsData/NTMSIDX"|mtime,md5|
C|"/mnt/hda1/WINNT/system32/nvModes.001"|mtime|
C|"/mnt/hda1/WINNT/system32/wbem/Logs/wbemcore.log"|mtime,size,md5|
C|"/mnt/hda1/WINNT/system32/wbem/Logs/WinMgmt.log"|mtime,size,md5|
C|"/mnt/hda1/WINNT/system32/wbem/Repository/$WinMgmt.CFG"|mtime|
C|"/mnt/hda1/WINNT/system32/wbem/Repository/CIM.REC"|mtime,size,md5|
C|"/mnt/hda1/WINNT/system32/wbem/Repository/CIM.REP"|mtime,md5|
C|"/mnt/hda1/WINNT/system32/wbem/Repository"|mtime|
C|"/mnt/hda1/WINNT/system32"|mtime|
C|"/mnt/hda1/WINNT/SchedLgU.Txt"|mtime,size,md5|
C|"/mnt/hda1/WINNT/ShellIconCache"|mtime,md5|
C|"/mnt/hda1/WINNT/CSC/00000001"|mtime|
N|"/mnt/hda1/WINNT/DASShp.dll"||
C|"/mnt/hda1/WINNT/Debug/ipsecpa.log"|mtime|
C|"/mnt/hda1/WINNT/Debug/ipsecpa.log.last"|mtime|
C|"/mnt/hda1/WINNT/Debug/oakley.log"|mtime|
C|"/mnt/hda1/WINNT/Debug/oakley.log.sav"|mtime|
C|"/mnt/hda1/WINNT/Debug/PASSWD.LOG"|mtime|
C|"/mnt/hda1/WINNT/Debug"|mtime|
C|"/mnt/hda1/WINNT"|mtime|
```

In this report we see most of the changes are to log files and other objects we would expect to change during normal operations. However, there are several new executables in a new folder called "C:/Program Files/Microsoft Reader/". This indicates the presence of new software on the system.

3.3 Verify The Security Configuration Against The Security Template.

We must now verify that the system security configuration is in compliance with the baseline. Since the baseline security configuration is contained in the organizational security template, it is relatively easy to detect any differences using the Microsoft Management Console (MMC) Security Configuration and Analysis snap-in.

Security Analysis Procedure.

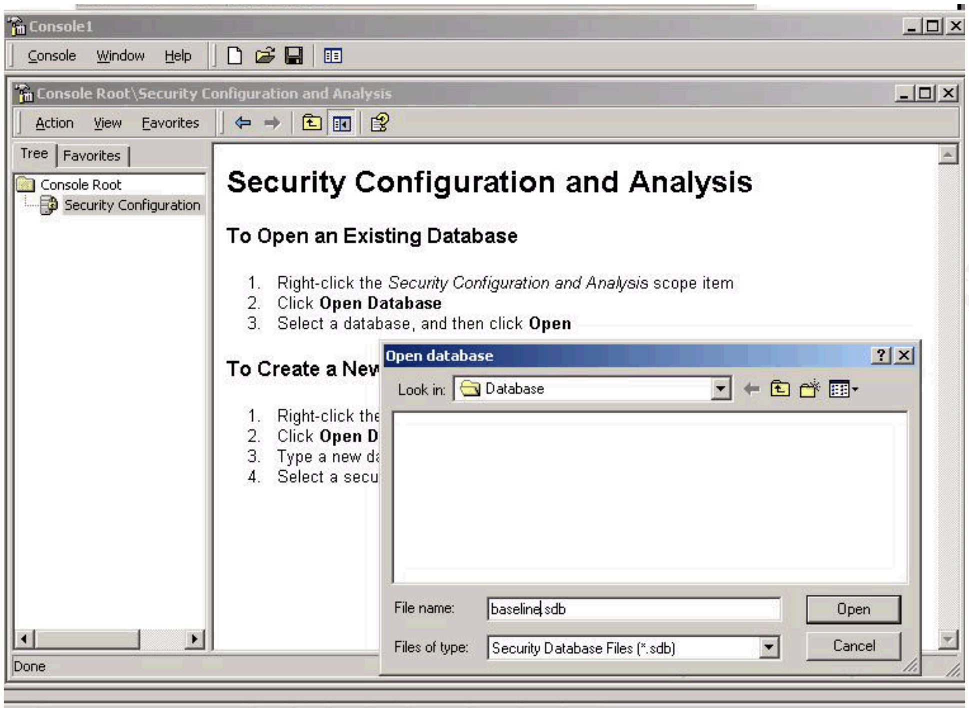
1) Boot the system under Windows 2000 and log in as the administrator.

2) Inset the USB drive with the organizational security template "orgtemplate.inf" into the USB port on the system.

3) Start the Microsoft Management Console: Start => Run => MMC.exe

4) Add the Security Configuration and Analysis Snap-in to the console.
-Click on the Console menu and select 'Add/Remove Snap-in'
-On the Add/Remove Snap-in dialog, click the Add button
-On the Add Standalone Snap-in dialog, select 'Security Configuration and Analysis' and click Add. Then click Close
-On the Add/Remove Snap-in dialog, click the OK button.

5) Create a new security database from the organizational security template.
-Right-click on 'Security Configuration and Analysis' in the Tree pane of the Console window. Enter new database name "baseline.sdb" and click Open.



Security Configuration and Analysis

To Open an Existing Database

1. Right-click the *Security Configuration and Analysis* scope item
2. Click **Open Database**
3. Select a database, and then click **Open**

To Create a New

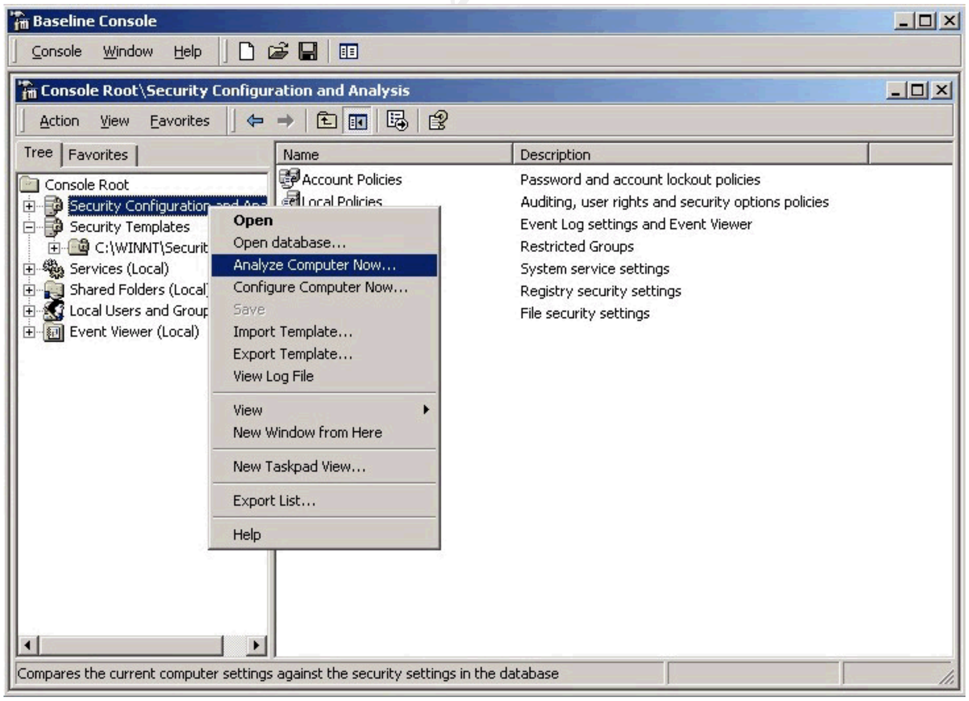
1. Right-click the
2. Click **Open D**
3. Type a new da
4. Select a secu

File name: baseline.sdb

Files of type: Security Database Files (*.sdb)

-On the Import Template dialog, navigate to the organizational template on the USB drive, probably D:\orgtemplate.inf, and click Open.

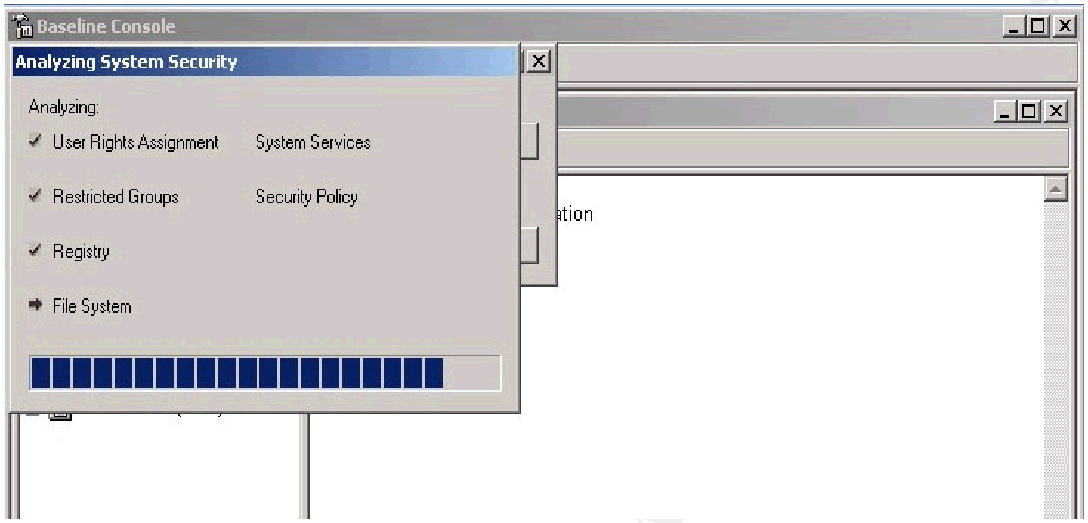
6) Start the analysis. Right-click on 'Security Configuration and Analysis' in the Tree pane of the Console window. Select 'Analyze Computer Now'. Click OK to confirm the error log path.



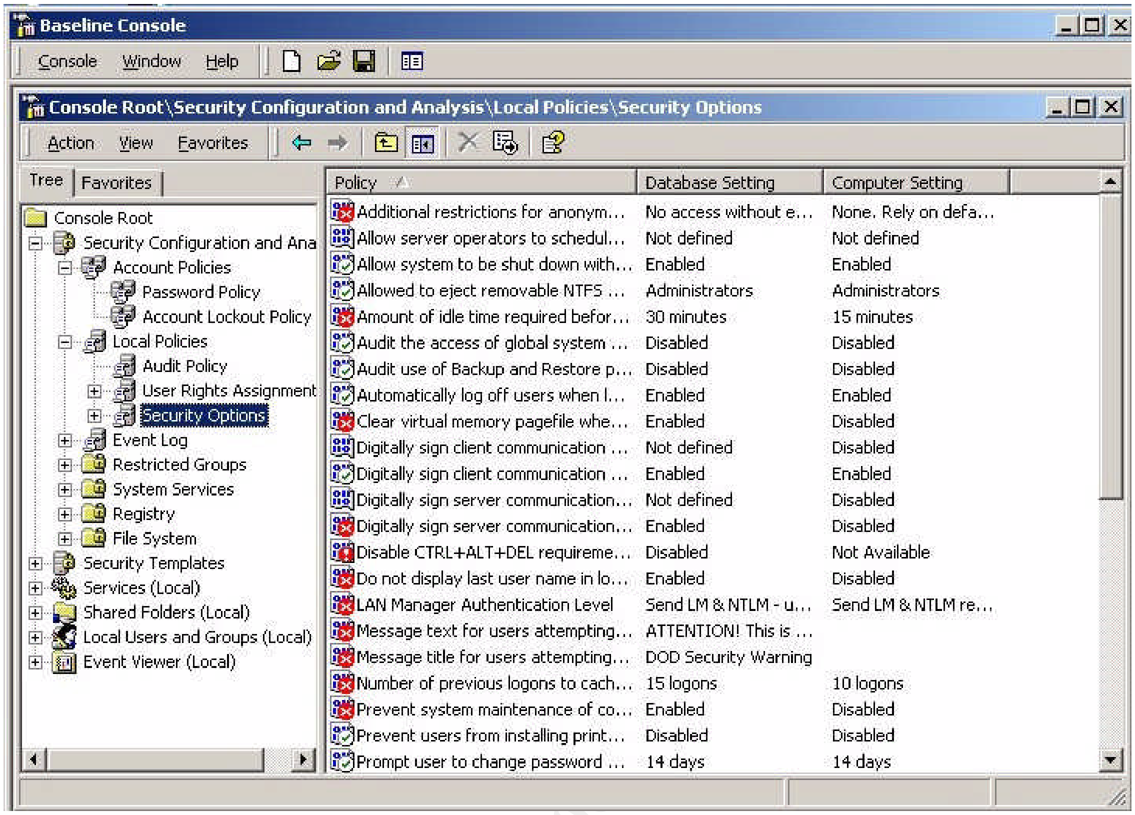
Name	Description
Account Policies	Password and account lockout policies
Local Policies	Auditing, user rights and security options policies
	Event Log settings and Event Viewer
	Restricted Groups
	System service settings
	Registry security settings
	File security settings

Compares the current computer settings against the security settings in the database

The snap-in will analyze the current settings in the systems security database against the settings in the "baseline.sdb" database, which now contains the settings from the organizational template.



7) Review the analysis results. Expand each of the items under Security Configuration and Analysis. The snap-in will make any settings that are not identical in the system configuration and the baseline configuration with a red X icon.



Policy	Database Setting	Computer Setting
Additional restrictions for anonym…	No access without e…	None. Rely on defa…
Allow server operators to schedul…	Not defined	Not defined
Allow system to be shut down with…	Enabled	Enabled
Allowed to eject removable NTFS …	Administrators	Administrators
Amount of idle time required befor…	30 minutes	15 minutes
Audit the access of global system …	Disabled	Disabled
Audit use of Backup and Restore p…	Disabled	Disabled
Automatically log off users when l…	Enabled	Enabled
Clear virtual memory pagefile whe…	Enabled	Disabled
Digitally sign client communication …	Not defined	Disabled
Digitally sign client communication …	Enabled	Enabled
Digitally sign server communication…	Not defined	Disabled
Digitally sign server communication…	Enabled	Disabled
Disable CTRL+ALT+DEL requireme…	Disabled	Not Available
Do not display last user name in lo…	Enabled	Disabled
LAN Manager Authentication Level	Send LM & NTLM - u…	Send LM & NTLM re…
Message text for users attempting…	ATTENTION! This is …	
Message title for users attempting…	DOD Security Warning	
Number of previous logons to cach…	15 logons	10 logons
Prevent system maintenance of co…	Enabled	Disabled
Prevent users from installing print…	Disabled	Disabled
Prompt user to change password …	14 days	14 days

Any mismatches should be investigated. The majority of these settings can only be changed by a user with administrator privileges. Thus changes could indicate successful privilege escalation attach or the presence of malicious software running in the SYSTEM context. The security event log may have an entry that recorded when the setting was changed and by whom.

3.4 Verify Other Security Settings.

The next step is to review the security items and settings that are not included in the security template. First, we will create a Microsoft Baseline Security Analyzer report for the system and compare the results against the baseline.

Run the Microsoft Baseline Security Analyzer against the local system, using the same procedures from section 2.5. The expected values are the same as the baseline MBSA report detailed in section 2.5. Any differences in these settings should be investigated.

Next we check that the Symantec Client Security suite is still configured correctly and operational.

Item / Expected Value	Procedure

Start up / Symantec Client Security runs on start up.	-Open the Windows Task Manager and go to the Processes tab. Observe that the following process are running: DefWatch.exe Rtvscan.exe SNDSrvc.exe SymSPort.exe VPTray.exe VPC32.exe -Any missing process could indicate a portion of the Symantec suite is not functioning normally.
File System Auto-protect / Enabled for all file types.	-Start => Programs => Symantec Client Security=> Symantec Antivirus. -Click the Configure menu and select File System Auto-protect. -Observe that the 'Enable Auto-Protect' check box is checked and that the 'All types' radio button is selected.
Internet E-mail Auto-protect / Enabled for all file types	-Click the Configure menu and select Internet E-mail Auto-protect. -Observe that the 'Enable Internet E-mail Auto-Protect' check box is checked and that the 'All types' radio button is selected.
Microsoft Exchange Auto-protect / Enabled for all file types.	-Click the Configure menu and select Microsoft Exchange Auto-protect. -Observe that the Microsoft Exchange Auto-protect ' check box is checked and that the 'All types' radio button is selected.
Update Schedule (Live Update) / Daily updates.	-Click the File menu and select Schedule Updates. -Observe that the 'Enable scheduled automatic updates' check box is checked and the text box reads "Update virus definitions every day at 8:00 PM"
Scheduled Scans / Weekly full system scan.	Expand the 'Scheduled Scans' sub-tree. -Click the entry titled 'Weekly Scan' -Observe that the Schedule text box reads: "Perform scan every Saturday at 2:00 AM" -Click Edit and observe that the Files tab shows 'My Computer' and all drives are selected for scanning.

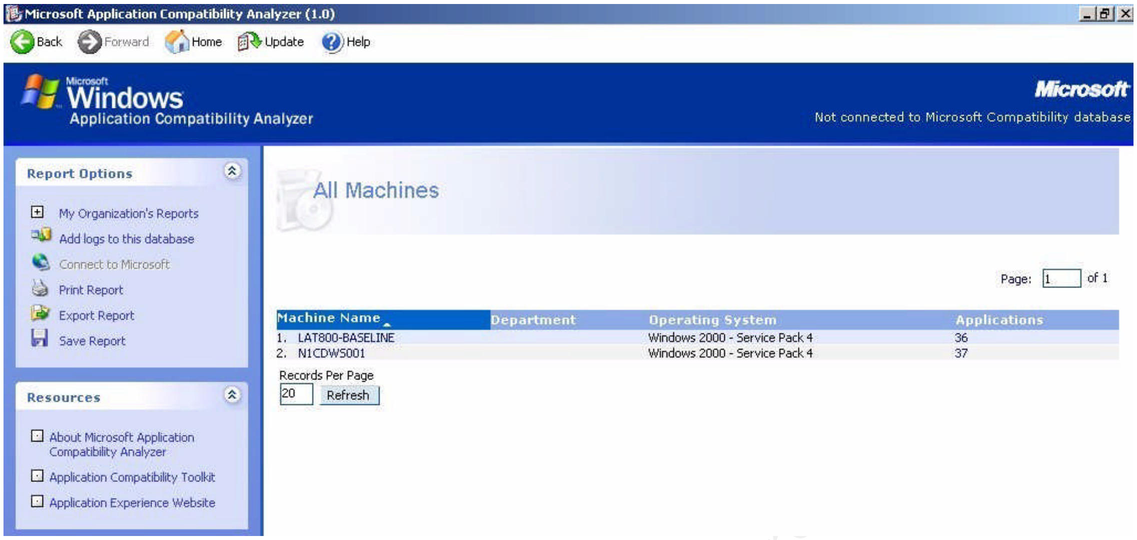
Client Firewall Configuration / Turned on and set to 'high'.	-Start => Programs => Symantec Client Security=> Symantec Client Firewall -Click on Client Firewall and the Configure button. -Observe that the 'Turn on Client Firewall' check box is checked and that the 'Firewall level' slider is set to 'High'.
Client Firewall Configuration / No entries in the 'Trusted' zone	-Click on the Networking tab -Observe that there are no entries in the trusted zone. -Click OK
Intrusion Detection Configuration / Turned on with AutoBlock turned on.	-Click Intrusion Detection and the Configure button -Observe that the 'Turn on Intrusion Detection' and 'Turn on AutoBlock' check boxes are checked. -Click Exclusions and observe that there are no entries in the 'Excluded Computers' text box. -Click OK and click OK.
Privacy Control / Turned on, medium level.	-Click Privacy Control and the Configure button. -Observe that the 'Turn on Privacy Control' check box is checked and that the Privacy Control level slider is set to medium. -Click OK.

3.5 Inventory The Installed Software.

Run Microsoft Application Compatibility Analyzer to check installed software against the baseline inventory. Use the procedures from section 2.6 to collect a MACA report from the subject system. We will now have a copy of this report on the USB drive.

1) Connect the USB drive to trusted workstation with MACA.

2) Import the collected report into the MACA database.
-Launch the Microsoft Application Compatibility Analyzer on the trusted workstation..
-Click 'Start using the analyzer'.
-Click 'Open existing database'.
-Click Continue
-Select 'All Machines'. The list of available reports is shown, this includes the baseline report.


Microsoft Application Compatibility Analyzer (1.0)
Back
Forward
Home
Update
Help
Microsoft Windows
Application Compatibility Analyzer
Microsoft
Not connected to Microsoft Compatibility database
Report Options
My Organization's Reports
Add logs to this database
Connect to Microsoft
Print Report
Export Report
Save Report
Resources
About Microsoft Application Compatibility Analyzer
Application Compatibility Toolkit
Application Experience Website
All Machines
Page: 1 of 1
Records Per Page
20
Refresh

Machine Name	Department	Operating System	Applications
1. LAT800-BASELINE		Windows 2000 - Service Pack 4	36
2. N1CDWS001		Windows 2000 - Service Pack 4	37

-Click 'Add logs to this database' from the left pane.

-'Specify Collector Log File Location' page, if the path to the USB drive is not shown, click the 'Add' button. Browse to find the USB drive and click OK.

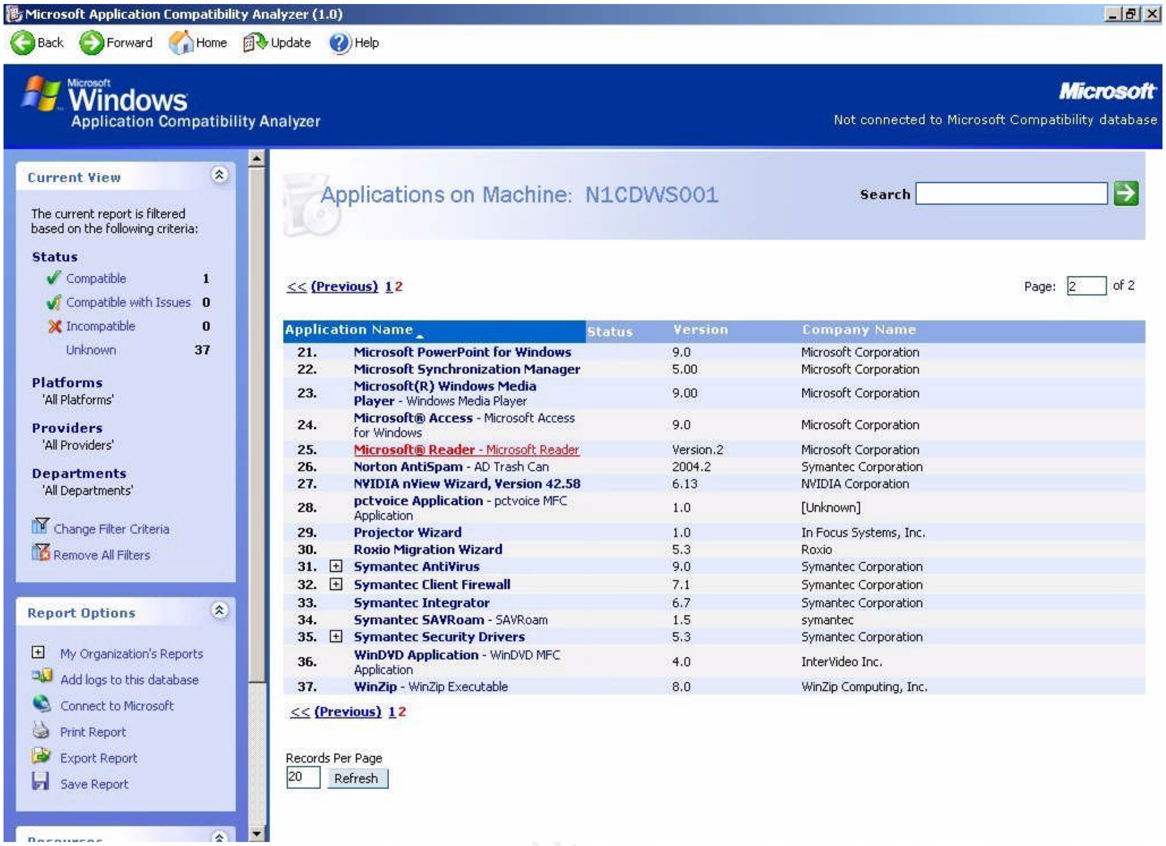
-Click Continue.

-'Connect to the Compatibility Database at Microsoft' click the 'No' radio button and then Continue. This information is not needed for a simple software inventory.

-The collector log file will be read from the USB drive. Click the Start button on the page to add this information to the database.

3) Review the report. We would expect the list to be identical to the baseline list. Any software changes from the baseline report should be investigated.

The example report shows that Microsoft Reader is present on the system. This is not part of the baseline software inventory. This confirms the file system map differences discovered by FTimes.



Applications on Machine: N1CDWS001

<< (Previous) 1 2 Page: 2 of 2

Application Name		Status	Version	Company Name
21.	Microsoft PowerPoint for Windows		9.0	Microsoft Corporation
22.	Microsoft Synchronization Manager		5.00	Microsoft Corporation
23.	Microsoft(R) Windows Media Player - Windows Media Player		9.00	Microsoft Corporation
24.	Microsoft® Access - Microsoft Access for Windows		9.0	Microsoft Corporation
25.	Microsoft® Reader - Microsoft Reader		Version.2	Microsoft Corporation
26.	Norton AntiSpam - AD Trash Can		2004.2	Symantec Corporation
27.	NVIDIA nView Wizard, Version 42.58		6.13	NVIDIA Corporation
28.	pctvoice Application - pctvoice MFC Application		1.0	[Unknown]
29.	Projector Wizard		1.0	In Focus Systems, Inc.
30.	Roxio Migration Wizard		5.3	Roxio
31.	⊞ Symantec AntiVirus		9.0	Symantec Corporation
32.	⊞ Symantec Client Firewall		7.1	Symantec Corporation
33.	Symantec Integrator		6.7	Symantec Corporation
34.	Symantec SAVRoam - SAVRoam		1.5	symantec
35.	⊞ Symantec Security Drivers		5.3	Symantec Corporation
36.	WinDVD Application - WinDVD MFC Application		4.0	InterVideo Inc.
37.	WinZip - WinZip Executable		8.0	WinZip Computing, Inc.

<< (Previous) 1 2

Records Per Page: 20 Refresh

CONCLUSION

This paper has presented an efficient, low-cost method for creating a comprehensive baseline for Windows 2000 Professional computers. It has also demonstrated techniques for evaluating systems against the baseline. Moreover, we have shown that the built in Windows 2000 tools, an open-source tool, (Ftimes) and no-cost tools from software manufacturer (Microsoft Baseline Security Analyzer and Microsoft Application Compatibility Analyzer), combined with a bit of ingenuity, can make a quite effective audit tool kit.

REFERENCES

Bower, Ben, Dean Farrington and Chris Weber. Securing Windows 2000 Professional Using the Gold Standard Security Template. SANS Press, 2002.

Cogswell, Bryce and Mark Russinovich. "RootkitRevealer" Sysinternals Web Site. 24 March 2005.
<http://www.sysinternals.com/ntw2k/freeware/rootkitreveal.shtml>

Liang, Ric. "Inventory Software with Microsoft's Application Compatibility Analyzer." TechRepublic web site. 23 December 2004.
<http://techrepublic.com.com/5102-22-5490828.html >

Microsoft Corporation. "Step-by-Step Guide to a Common Infrastructure for Windows 2000 Server Deployment - Part 2: Installing a Windows 2000 Professional Workstation and Connecting It to a Domain." Microsoft Web Site. 21 January 21 2000. <http://www.microsoft.com/windows2000/techinfo/ planning/ server/prosteps.asp>

Microsoft Corporation. "Microsoft Windows 2000 Security Hardening Guide." Microsoft Web Site. 11 April 2003. <http://www.microsoft.com/technet/security/ prodtech/ windows2000/win2khg/default.mspx>

Microsoft Corporation. "White Paper: Microsoft Baseline Security Analyzer V1.2" Microsoft Web Site. 17 June 2004.
<http://www.microsoft.com/technet/security/tools/mbsawp.mspx>

Monroe, Klayton and Dave Bailey. "System Baselining - A Forensic Perspective." FTimes web site. 11 June 2002.
<http://ftimes.sourceforge.net/files/papers/baselining.pdf >

Monroe, Klayton. "FTimes Man Page." Source Forge web site. 2004
<http://ftimes.sourceforge.net/FTimes/ManPage.shtml>

Souppaya, Murugiah et al. Systems Administration Guidance for Securing Microsoft Windows 2000 Professional System, NIST Special Publication 800-43. Washington: National Institute of Standards and Technology, 2002.

Vibert, Robert. "Infectable Objects Part Two - Windows Infectable" Security Focus web site. 29 Sept 2000. <http://www.securityfocus.com/infocus/1273>

APPENDIX 1 Organizational Security Template

```
;------------------------------------------------------------------------------
; <organization> Windows 2000 Security Template
; 4 APR 03
;x Robert L. Fanelli, ...
;
; Windows 2000 Professional Security Settings
; NIST, NSA, DISA, SANS, and CIS
;
; ---------------------
; Security Configuration Template for Security Configuration Editor
;
; Template Name:        <organization>_Win2kProGold_R1.2.inf
; Template Version:     R1.2
; Date Created:         2002-11-21
; Date Last Modified:   2003-04-04
;
; Introduction:
; -------------
; This template introduces the Windows 2000 Professional security baseline that
; is based on the recommendations made by a NIST, NSA, SANS, and CIS.
; These settings have been reviewed and approved by DISA and GSA.
; This template is derived from the NSA, NIST,DISA, and Microsoft Windows
2000
; Professional templates with minor modifications.
;
; DISCLAIMER:
; -----------
; This template is provided as a resource for Windows 2000 Professional users.
It
; should not be implemented without examining its contents thoroughly first.
Those
; elements of this template that can possibly cause unpredictable behavior for
; Windows 2000 Professional are clearly noted. This template is not designed to
; cause any type of damage to any Windows 2000 Professional system in any
method
; what so ever.It is strongly recommended that these settings be reviewed to
; comply with local policy and tested on non-production systems before being
; deployed.
;
; More information:
; -----------------
; For more information consult the following Internet URLs
;
; http://csrc.nist.gov/itsec/guidance_W2Kpro.html
; http://nsa1.www.conxion.com/win2k/index.html
; http://iase.disa.mil/
; http://www.cisecurity.org/
; http://www.sans.org
; http://www.microsoft.com/windows2000
;
; Revision History:
; ----------------
; R1.0  Initial Release
; R1.1  Incorporate Microsoft Suggestions - Round 1
; R1.2  Incorporate Microsoft Suggestions - Round 2
;
; 4 APR 03: Adjusted LM Compatibility Level to DWORD,1
;
;-------------------------------------------------------------------------

; This is a description of this security template. Feel free to change the
; description to reflect and identify your specific organization

; Informs Windows 2000 Professional to use the Unicode character set. Please
note
; that there are issues with using Unicode, e.g. in an LAN environment where
ASCII
; is used by other clients.
; For more information consult the Unicode home page:
; http://www.unicode.org
[Unicode]
Unicode=yes

; This section defines parameters for account security and password policy.
They
; correspond to the Account policies section of the Local Security policy MMC
; snap-in.
[System Access]
MinimumPasswordAge = 1
MaximumPasswordAge = 90
MinimumPasswordLength = 8
PasswordComplexity = 1
PasswordHistorySize = 24
LockoutBadCount = 3
ResetLockoutCount = 15
LockoutDuration = 15
RequireLogonToChangePassword = 1
ForceLogoffWhenHourExpire = 1
ClearTextPassword = 0
```

```
; For each of the three log settings below, the default maximum size is 80MB
; on all three logs. Although logs may never actually reach their full size
; this setting should reflect the physical hard drive space that is available
; You should change this setting only if you are completly aware of the status
; of the physical log files in tandem with the audit policy of your enterprise.

; This section determines settings specific to the System Log They correspond
; to the Event Log section of the Security Configuration and  Analysis MMC
; snap-in.
[System Log]
MaximumLogSize = 81920
AuditLogRetentionPeriod = 0
RestrictGuestAccess = 1

; This section determines settings specific to the Security Log They correspond
; to the Event Log section of the Security Configuration and  Analysis MMC
; snap-in.
[Security Log]
MaximumLogSize = 81920
AuditLogRetentionPeriod = 0
RestrictGuestAccess = 1

; This section determines settings specific to the Application Log They
correspond
; to the Event Log section of the Security Configuration and  Analysis MMC
; snap-in.
[Application Log]
MaximumLogSize = 81920
AuditLogRetentionPeriod = 0
RestrictGuestAccess = 1

; This section determines overall audit policy, it corresponds to the Audit
; policy section of the MMC snap-in. The integers 0-3 correspond to values
; of not auditing particular event, Audit the event's Success, Audit the
; event's Failure or audit both types of outcomes for the event.
; 0 - Don't log anything for event
; 1 - Log event successes
; 2 - Log event failures
; 3 - Log both event successes and failures
[Event Audit]
AuditSystemEvents = 3
AuditLogonEvents = 3
AuditObjectAccess = 2
AuditPrivilegeUse = 2
AuditPolicyChange = 2
AuditAccountManage = 3
```

```
AuditAccountLogon = 3
CrashOnAuditFull = 0

[Version]
signature="$CHICAGO$"
Revision=1

; Privilege Rights correspond to the User Rights Assignment section of the
; Local Security Policy MMC snap-in. These rights are assigned to individual
; accounts or user groups that are defined. The following table lists the SIDS
; that are used below.
;                    SID Table:
; ----------------------------------------
;      SID         | Description
; ----------------------------------------
; *S-1-5-32-544  | Administrators Group
; ----------------------------------------
; *S-1-5-32-545  | Users group
; ----------------------------------------



; This section sets security for services

; This section details registry values to modify/add to Windows 2000
Professional.
; These values are designed to enhance the security of the operating system.
; The following table is taken from the Microsoft template hisecws.inf. It
describes
; the representations of the various registry data types.
;------------------------------------------------------------------
;Registry Values
;------------------------------------------------------------------
; Registry value name in full path = Type, Value
; REG_SZ                    ( 1 )
; REG_EXPAND_SZ             ( 2 )  // with environment variables to expand
; REG_BINARY                ( 3 )
; REG_DWORD                 ( 4 )
; REG_MULTI_SZ              ( 7 )
[Registry Keys]
"machine\software",2,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI
;KR;;;BU)"
"machine\software\microsoft\netdde",2,"D:PAR(A;CI;KA;;;BA)(A;CI;KA;;;SY)"
"MACHINE\SOFTWARE\Microsoft\OS/2 Subsystem for
NT",2,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)"
"machine\software\microsoft\protected storage system provider",1,"D:AR"
```

```
"machine\software\microsoft\windows\currentversion\group
policy",0,"D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CI;KA;;;SY)"
"machine\software\microsoft\windows\currentversion\installer",0,"D:PAR(A;CI;K
A;;;BA)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"machine\software\microsoft\windows\currentversion\policies",0,"D:PAR(A;CI;K
A;;;BA)(A;CI;KR;;;AU)(A;CI;KA;;;SY)"
"machine\system",2,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;
KR;;;BU)"
"machine\system\clone",1,"D:AR"
"machine\system\controlset001",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;
KA;;;SY)(A;CI;KR;;;BU)"
"machine\system\controlset002",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;
KA;;;SY)(A;CI;KR;;;BU)"
"machine\system\controlset003",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;
KA;;;SY)(A;CI;KR;;;BU)"
"machine\system\controlset004",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;
KA;;;SY)(A;CI;KR;;;BU)"
"machine\system\controlset005",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;
KA;;;SY)(A;CI;KR;;;BU)"
"machine\system\controlset006",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;
KA;;;SY)(A;CI;KR;;;BU)"
"machine\system\controlset007",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;
KA;;;SY)(A;CI;KR;;;BU)"
"machine\system\controlset008",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;
KA;;;SY)(A;CI;KR;;;BU)"
"machine\system\controlset009",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;
KA;;;SY)(A;CI;KR;;;BU)"
"machine\system\controlset010",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;
KA;;;SY)(A;CI;KR;;;BU)"
"machine\system\currentcontrolset\control\securepipeservers\winreg",2,"D:PAR(
A;CI;KA;;;BA)(A;;KR;;;BO)(A;CI;KA;;;SY)"
"machine\system\currentcontrolset\control\wmi\security",2,"D:P(A;CI;GR;;;BA)(A
;CI;GA;;;SY)(A;CI;GA;;;CO)"
"machine\system\currentcontrolset\enum",1,"D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU
)(A;CI;KA;;;SY)"
"machine\system\currentcontrolset\hardware
profiles",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"users\.default",2,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;
;;BU)"
"users\.default\software\microsoft\netdde",2,"D:PAR(A;CI;KA;;;BA)(A;CI;KA;;;SY
)"
"users\.default\software\microsoft\protected storage system provider",1,"D:AR"
"CLASSES_ROOT",2,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI
;KR;;;BU)"
"machine\software\microsoft\windows
nt\currentversion\perflib",2,"D:P(A;CI;GR;;;IU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;
GA;;;CO)"
"machine\software\Microsoft\Windows
NT\CurrentVersion\AsrCommands",2,"D:PAR(A;CI;KA;;;BA)(A;CI;CCDCLCSWR
PSDRC;;;BO)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\PermittedM
anagers",2,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)"
"MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\ValidCom
munities",2,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)"


; This section defines the permissions for files and folders that can be found on
Windows
; 2000 Professional. Please note that not all of these resources will be available
on all
; installations of Windows 2000 Professional
[File Security]
"%SystemRoot%\Debug\UserMode",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(
A;;CCDCWP;;;BU)(A;OIIO;DCLC;;;BU)"
"%SystemRoot%\system32\secedit.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;
SY)"
"%SystemDrive%\Documents and Settings\All
Users\Documents\DrWatson",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OI
CI;FA;;;SY)(A;OICIIO;DCLCWP;;;BU)(A;OICI;CCSWWPLORC;;;BU)"
"%SystemDrive%\Documents and
Settings\Administrator",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\system32\regedt32.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;
;SY)"
"%SystemRoot%\system32\rsh.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\system32\rexec.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY
)"
"%SystemRoot%\system32\Ntbackup.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;
;;SY)"
"%SystemRoot%\system32\rcp.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\regedit.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDrive%\MSDOS.SYS",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
"%SystemDrive%\IO.SYS",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
"%SystemDrive%\",0,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY
)(A;OICI;0x1200a9;;;BU)"
"%SystemDrive%\Temp",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;F
A;;;SY)(A;CI;DCLCWP;;;BU)"
"%SystemDrive%\Documents and
Settings",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemRoot%\system32\ias",2,"D:P(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;
GA;;;CO)"
"%SystemRoot%\system32\dllcache",2,"D:P(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A
;OICI;GA;;;CO)"
```

```
"%SystemRoot%\config",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\system32\spool\printers",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;CI;DCLCSWWPLO;;;BU)"
"%SystemRoot%\ReinstallBackups",1,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;0x1200a9;;;PU)(A;OICI;FA;;;SY)"
"%SystemRoot%\system32\Setup",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemRoot%\system32\NTMSData",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\system32\GroupPolicy",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(A;OICI;FA;;;SY)"
"%SystemRoot%\system32\DTCLog",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemRoot%\system32\appmgmt",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemRoot%",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemRoot%\Temp",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;CI;0x100026;;;BU)"
"%SystemRoot%\Tasks",2,"D:AR"
"%SystemRoot%\repair",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\Registration",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;FR;;;BU)"
"%SystemRoot%\debug",0,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemRoot%\CSC",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%ProgramFiles%",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"c:\config.sys",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
"c:\autoexec.bat",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
; cannot find
;"c:\ntbootdd.sys",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
"c:\ntldr",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
"c:\ntdetect.com",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
"c:\boot.ini",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
"%SystemRoot%\$NtServicePackUninstall$",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDrive%\Documents and Settings\All Users",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemRoot%\Offline Web Pages",2,"D:(A;OICI;GA;;;WD)"
"%SystemDrive%\autoexec.bat",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
"%SystemDrive%\boot.ini",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDrive%\ntdetect.com",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDrive%\config.sys",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
```

```
"%SystemDrive%\ntldr",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDrive%\Documents and Settings\Default
User",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemRoot%\security",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;
FA;;;SY)"
"%SystemDrive%\Program Files\Resource
Kit",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\system32\at.exe",1,"D:PAR(A;OICI;FA;;;LA)"
[Privilege Rights]
seassignprimarytokenprivilege =
seauditprivilege =
sebackupprivilege = *S-1-5-32-547,*S-1-5-32-544
sebatchlogonright =
sechangenotifyprivilege = *S-1-5-32-545
secreatepagefileprivilege = *S-1-5-32-544
secreatepermanentprivilege =
secreatetokenprivilege =
sedebugprivilege =
sedenybatchlogonright =
sedenyinteractivelogonright = *S-1-5-32-546
sedenynetworklogonright = *S-1-5-32-546
sedenyservicelogonright =
seenabledelegationprivilege =
seincreasebasepriorityprivilege = *S-1-5-32-544
seincreasequotaprivilege = *S-1-5-32-544
seinteractivelogonright = *S-1-5-32-545,*S-1-5-32-547,*S-1-5-32-544
seloaddriverprivilege = *S-1-5-32-547,*S-1-5-32-544
selockmemoryprivilege =
semachineaccountprivilege =
senetworklogonright = *S-1-5-32-545,*S-1-5-32-547,*S-1-5-32-544
seprofilesingleprocessprivilege = *S-1-5-32-544
seremoteshutdownprivilege = *S-1-5-32-544
serestoreprivilege = *S-1-5-32-544
sesecurityprivilege = *S-1-5-32-544
seservicelogonright =
seshutdownprivilege = *S-1-5-32-545,*S-1-5-32-547,*S-1-5-32-544
sesyncagentprivilege =
sesystemenvironmentprivilege = *S-1-5-32-544
sesystemprofileprivilege = *S-1-5-32-544
sesystemtimeprivilege = *S-1-5-32-545,*S-1-5-32-547,*S-1-5-32-544
setakeownershipprivilege = *S-1-5-32-544
setcbprivilege =
seundockprivilege = *S-1-5-32-545,*S-1-5-32-547,*S-1-5-32-544
[Service General Setting]
Messenger,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)S:(AU;F
A;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
```

```
ClipSrv,3,"D:(A;OICI;CCLCSWLORC;;;WD)(A;OICI;CCDCLCSWRPWPDTLOCR
SDRCWDWO;;;BA)(A;OICI;CCLCSWLORC;;;PU)(A;OICI;CCLCSWRPLO;;;IU)S:
(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
RemoteAccess,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)"
Browser,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)S:(AU;FA;
CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
ClipSrv,4,"D:AR(A;OICI;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)S:(AU;
FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
RemoteAccess,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)"
TlntSvr,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)"
SharedAccess,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)"
Alerter,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)"
Fax,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)"
MSFTPSVC,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)"
IISADMIN,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)"
mnmsrvc,3,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)"
RemoteRegistry,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)"
SMTPSVC,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)"
SNMP,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)"
SNMPTRAP,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)"
W3SVC,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)"
wuauserv,2,"D:(A;OICI;GA;;;WD)"
RSVP,3,"D:(A;OICI;GA;;;WD)"
NetDDE,4,"D:(A;OICI;GA;;;WD)"
NetDDEdsdm,4,"D:(A;OICI;GA;;;WD)"
seclogon,3,"D:(A;OICI;GA;;;WD)"
[Registry Values]
MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet
Settings\ProxySettingsPerUser=4,0
MACHINE\Software\Microsoft\Office\9.0\Outlook\Security\SupressNameChecks
=4,0
MACHINE\Software\Microsoft\Office\9.0\Outlook\Security\EnableSRFeatures=4,
1
machine\system\CurrentControlSet\Services\IPSEC\NoDefaultExempt=4,1
machine\system\CurrentControlSet\Services\Tcpip\Parameters\EnablePMTUDis
covery=4,1
machine\system\CurrentControlSet\Services\Tcpip\Parameters\EnableICMPRed
irect=4,0
machine\system\CurrentControlSet\Services\Tcpip\Parameters\EnableDeadGW
Detect=4,0
machine\system\CurrentControlSet\Services\Tcpip\Parameters\KeepAliveTime=
4,300000
machine\system\CurrentControlSet\Services\Tcpip\Parameters\DisableIPSource
Routing=4,2
machine\system\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxHalfOpe
nRetried=4,80
```

```
machine\system\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxHalfOpen=4,100
machine\system\CurrentControlSet\Services\Tcpip\Parameters\SynAttackProtect=4,1
machine\system\CurrentControlSet\Services\Tcpip\Parameters\PerformRouterDiscovery=4,0
machine\system\CurrentControlSet\Services\Tcpip\Parameters\NoNameReleaseOnDemand=4,1
machine\System\CurrentControlSet\Services\LanmanServer\Parameters\AutoShareWks=4,0
machine\system\CurrentControlSet\Services\Cdrom\Autorun=4,0
machine\system\CurrentControlSet\Services\MrxSmb\Parameters\RefuseReset=4,1
machine\system\CurrentControlSet\Control\CrashControl\AutoReboot=4,0
machine\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun=4,255
machine\Software\Microsoft\Windows\CurrentVersion\Policies\NetworkHideSharePwds=4,1
machine\Software\Microsoft\Windows\CurrentVersion\Policies\NetworkNoDialIn=4,1
machine\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SFCShowProgress=4,0
machine\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SFCScan=4,0
machine\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\DontDisplayLastUserName=1,1
machine\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AeDebug\Auto=4,0
machine\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SFCDisable=4,4
machine\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AutoAdminLogon=1,0
machine\SOFTWARE\Microsoft\DrWatson\CreateCrashDump=4,0
machine\SOFTWARE\Microsoft\Command Processor\PathCompletionChar=4,9
machine\system\CurrentControlSet\Control\Lsa\RestrictAnonymous=4,2
machine\system\currentcontrolset\services\netlogon\parameters\signsecurechannel=4,1
machine\system\currentcontrolset\services\netlogon\parameters\sealsecurechannel=4,1
machine\system\currentcontrolset\services\netlogon\parameters\disablepasswordchange=4,1
machine\system\currentcontrolset\services\lanmanworkstation\parameters\enablesecuritysignature=4,1
machine\system\currentcontrolset\services\lanmanworkstation\parameters\enableplaintextpassword=4,0
machine\system\currentcontrolset\services\lanmanserver\parameters\enablesec
```

```
uritysignature=4,1
machine\system\currentcontrolset\services\lanmanserver\parameters\enableforc
edlogoff=4,1
machine\system\currentcontrolset\services\lanmanserver\parameters\autodisco
nnect=4,30
machine\system\currentcontrolset\control\session manager\protectionmode=4,1
machine\system\currentcontrolset\control\session manager\memory
management\clearpagefileatshutdown=4,1
machine\system\currentcontrolset\control\print\providers\lanman print
services\servers\addprinterdrivers=4,0
machine\system\currentcontrolset\control\lsa\lmcompatibilitylevel=4,1
machine\software\microsoft\windows\currentversion\policies\system\shutdownw
ithoutlogon=4,1
machine\software\microsoft\windows\currentversion\policies\system\dontdisplay
lastusername=4,1
machine\software\microsoft\windows\currentversion\policies\system\disablecad
=4,0
machine\software\microsoft\windows
nt\currentversion\winlogon\scremoveoption=1,1
machine\software\microsoft\windows
nt\currentversion\winlogon\passwordexpirywarning=4,14
machine\software\microsoft\windows
nt\currentversion\winlogon\cachedlogonscount=1,15
machine\software\microsoft\windows
nt\currentversion\winlogon\allocatefloppies=1,1
machine\software\microsoft\windows
nt\currentversion\winlogon\allocatedasd=1,0
machine\software\microsoft\windows
nt\currentversion\setup\recoveryconsole\setcommand=4,0
machine\software\microsoft\windows
nt\currentversion\setup\recoveryconsole\securitylevel=4,0
machine\software\microsoft\non-driver signing\policy=3,1
machine\software\microsoft\driver signing\policy=3,1
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalN
oticeText=1,ATTENTION! This is a <organization> computer system.  Before
processing classified information,check the security accreditation level of this
system. Do NOT process,store,or transmit information classified above the
accreditation level of this system. This computer system,including all related
equipment,networks,and network devices (includes internet access) are
provided only for authorized <organization>. <organization> computer systems
may be monitored for all lawful purposes,including to ensure their use is
authorized,for management of the system,to facilitate protection against
unauthorized access,and to verify security procedures,survivability,and
operational security,monitoring includes,but is not limited to,active attacks by
authorized <organization> entities to test or verify the security of this system.
During monitoring,information may be examined,recorded,copied,and used for
```

```
authorized purposes. All information,including personal information,placed on or
sent over this system may be monitored. use of this <organization> computer
system,authorized or unauthorized,constitutes consent to monitoring.
Unauthorized use of this <organization> computer system may subject you to
criminal prosecution.  Evidence of unauthorized use collected during monitoring
may be used for administrative,criminal,or other adverse action.  Use of this
system constitutes consent to monitoring for all lawful purposes.
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalN
oticeCaption=1, * Security Warning *
MACHINE\System\CurrentControlSet\Control\Lsa\AuditBaseObjects=4,0
MACHINE\System\CurrentControlSet\Control\Lsa\FullPrivilegeAuditing=3,0
machine\system\currentcontrolset\services\lanmanserver\parameters\hidden=4,
1
MACHINE\System\CurrentControlSet\Control\Lsa\CrashOnAuditFail=4,0
[Profile Description]
Description= <organization> Windows 2000 Professional Security Settings,
APR 2003
```

APPENDIX 2 Extract of FTimes Map File

```
name|dev|inode|mode|nlink|uid|gid|rdev|mtime|ctime|size|magic|md5
"/mnt/hda1/arcldr.exe"|769|2677|100400|1|1000|1000|0|2003-06-19
19:05:04|2005-03-15 00:30:38|150528||ae30898396b11ea379c7bd15316bd3c6
"/mnt/hda1/arcsetup.exe"|769|2678|100400|1|1000|1000|0|2003-06-19
19:05:04|2005-03-15 00:30:38|163840||51b4110935a5620483cae8b86c8d2371
"/mnt/hda1/AUTOEXEC.BAT"|769|4366|100400|1|1000|1000|0|2005-02-23
19:03:11|2005-03-15 00:30:38|0||d41d8cd98f00b204e9800998ecf8427e
"/mnt/hda1/boot.ini"|769|2716|100400|1|1000|1000|0|2005-02-23 09:11:19|2005-
03-15 00:30:38|192||bec50a347a5fb2ff498be5022637180f
"/mnt/hda1/CONFIG.SYS"|769|4362|100400|1|1000|1000|0|2005-02-23
19:03:11|2005-03-15 00:30:38|0||d41d8cd98f00b204e9800998ecf8427e
"/mnt/hda1/IO.SYS"|769|4367|100400|1|1000|1000|0|2005-02-23 19:03:11|2005-
03-15 00:30:39|0||d41d8cd98f00b204e9800998ecf8427e
"/mnt/hda1/lockdown.txt"|769|13385|100400|1|1000|1000|0|2005-03-15
00:31:15|2005-03-15 00:32:51|6879||f5a461bb84699506a705757dca575015
"/mnt/hda1/MSDOS.SYS"|769|4368|100400|1|1000|1000|0|2005-02-23
19:03:11|2005-03-15 00:30:39|0||d41d8cd98f00b204e9800998ecf8427e
"/mnt/hda1/NTDETECT.COM"|769|2683|100400|1|1000|1000|0|2005-02-25
19:45:03|2005-03-15 00:30:39|34724||21d9176d8dba084b0b6f2a0159aeeb83
"/mnt/hda1/ntldr"|769|2679|100400|1|1000|1000|0|2005-02-25 19:45:03|2005-03-
15 00:30:39|214432||2ecc0cd4197c012f9d0fcff7f78e1d34
"/mnt/hda1/nvlog.txt"|769|399|100400|1|1000|1000|0|2005-03-14 19:32:53|2005-
03-15 00:30:38|0||d41d8cd98f00b204e9800998ecf8427e
"/mnt/hda1/office-sr1/ART.msp"|769|11171|100400|1|1000|1000|0|2000-05-03
01:29:04|2005-03-15 00:30:38|8410624||ac006caaa968673976d7db381d33dced
"/mnt/hda1/office-sr1/autorun.inf"|769|9250|100400|1|1000|1000|0|2000-02-07
06:20:38|2005-03-15 00:30:38|47||f74299f588f33a6c45c520aec7252354
"/mnt/hda1/office-sr1/data1.msp"|769|9252|100400|1|1000|1000|0|2000-05-03
01:26:44|2005-03-15
00:30:38|27412992||4629cdb62bac292216d47d77c7a9254c
"/mnt/hda1/office-sr1/data2.msp"|769|9253|100400|1|1000|1000|0|2000-05-03
01:29:34|2005-03-15
00:30:38|13695488||71c276e046290e75de5f9c93172bb034
"/mnt/hda1/office-sr1/fpse.msp"|769|9254|100400|1|1000|1000|0|2000-03-07
04:42:30|2005-03-15 00:30:38|739328||fb1303c3020c2105aee6e95c3d788ffd
"/mnt/hda1/office-sr1/Instmsi.exe"|769|9255|100400|1|1000|1000|0|2000-02-01
20:13:22|2005-03-15 00:30:38|1857280||d155aa1f54f14fa530481f5561bf1275
"/mnt/hda1/office-sr1/Instmsiw.exe"|769|11122|100400|1|1000|1000|0|2000-02-
01 20:15:10|2005-03-15
00:30:38|1878784||8c226a2a8a9958a56d731a606ca72d27
"/mnt/hda1/office-sr1/O9sr1.hlp"|769|11167|100400|1|1000|1000|0|2000-02-07
06:20:42|2005-03-15 00:30:38|7932||4c5c5204f5a2a313b957d36d0b68a97e
"/mnt/hda1/office-sr1/ows.msp"|769|11168|100400|1|1000|1000|0|2000-02-28
```

```
20:20:06|2005-03-15 00:30:38|7765504||d875fdf40497cdd3b282d5c1583c1f1e
"/mnt/hda1/office-sr1/Readme.doc"|769|11169|100400|1|1000|1000|0|2000-02-
26 05:15:00|2005-03-15 00:30:38|14336||8dbc96c6f5c7e44428e555ae5c056f84
"/mnt/hda1/office-sr1/setup.exe"|769|11170|100400|1|1000|1000|0|2000-03-10
04:00:56|2005-03-15 00:30:38|233472||ae38da0801399de3d7d2adf1a3a748c1
"/mnt/hda1/office-sr1/source.ini"|769|9249|100400|1|1000|1000|0|2000-05-05
18:04:48|2005-03-15 00:30:38|5052||8421793f6329b4d1a58ccae0e390d1cf
"/mnt/hda1/office-sr1"|769|9248|40500|1|1000|1000|0|2005-02-25 20:45:36|2005-
03-15 00:30:38|4096||DIRECTORY
"/mnt/hda1/pagefile.sys"|769|24|100400|1|1000|1000|0|2005-03-15
00:50:52|2005-03-15
00:50:52|1610612736||2c849621761711823e6620de16d8436f
"/mnt/hda1/Program+Files/3Com"|769|7187|40500|1|1000|1000|0|2005-02-23
19:31:50|2005-03-15 00:30:39|0||DIRECTORY
"/mnt/hda1/Program+Files/Accessories/Imagevue"|769|3566|40500|1|1000|1000
|0|2005-02-23 09:13:10|2005-03-15 00:30:39|0||DIRECTORY
"/mnt/hda1/Program+Files/Accessories"|769|3565|40500|1|1000|1000|0|2005-02-
23 09:13:10|2005-03-15 00:30:39|0||DIRECTORY
"/mnt/hda1/Program+Files/Adobe/Acrobat+6.0/Esl/AiodLite.dll"|769|11589|1004
00|1|1000|1000|0|2003-11-04 00:17:06|2005-03-15
00:30:39|28672||2ad816e92aaa36a8efc74e7166de11d7
"/mnt/hda1/Program+Files/Adobe/Acrobat+6.0/Esl"|769|11588|40500|1|1000|10
00|0|2005-03-11 01:50:29|2005-03-15 00:30:39|0||DIRECTORY
"/mnt/hda1/Program+Files/Adobe/Acrobat+6.0/Help/ENU/Reader.pdf"|769|1184
4|100400|1|1000|1000|0|2003-11-03 23:24:04|2005-03-15
00:30:39|1555307||47bd0c76ffd7d57f64656b560cd539a0
"/mnt/hda1/Program+Files/Adobe/Acrobat+6.0/Help/ENU"|769|11843|40500|1|1
000|1000|0|2005-03-11 01:50:31|2005-03-15 00:30:39|0||DIRECTORY
"/mnt/hda1/Program+Files/Adobe/Acrobat+6.0/Help"|769|11842|40500|1|1000|1
000|0|2005-03-11 01:50:31|2005-03-15 00:30:39|0||DIRECTORY
"/mnt/hda1/Program+Files/Adobe/Acrobat+6.0/Reader/Ace.dll"|769|11825|1004
00|1|1000|1000|0|2003-05-02 01:34:04|2005-03-15
00:30:39|565248||419549bb6920b5fb13526030d1559a9d
"/mnt/hda1/Program+Files/Adobe/Acrobat+6.0/Reader/Acrofx32.dll"|769|11833|1
00400|1|1000|1000|0|2003-05-15 09:47:20|2005-03-15
00:30:39|53248||9cec69ddaa71cc138fc4181ec88028aa
"/mnt/hda1/Program+Files/Adobe/Acrobat+6.0/Reader/AcroRd32.exe"|769|1182
4|100400|1|1000|1000|0|2003-11-04 00:49:24|2005-03-15
00:30:39|7671876||572f64072ee4abe6dd7f217e22fd6e31
"/mnt/hda1/Program+Files/Adobe/Acrobat+6.0/Reader/ActiveX/AcroIEHelper.dll"
|769|11585|100400|2|1000|1000|0|2003-11-04 00:17:44|2005-03-15
00:30:39|54248||fc7850324464e4d19a24a03d882b5cc4
"/mnt/hda1/Program+Files/Adobe/Acrobat+6.0/Reader/ActiveX/GbDetect.dll"|76
9|11523|100400|1|1000|1000|0|2003-11-04 00:32:54|2005-03-15
00:30:39|86016||ba365dae49db6b682af9665a7bfd237e               <snip>
```