# Global Information Assurance Certification Paper

# Registry Key Security
## Practical Assignment for GIAC Monterey 2000
## Windows Security

Submitted by: Daniel A Boss

# Table of Contents

Windows system security and hardening best practices are based upon a layered approach consisting of operating system changes, file and directory permission modifications, registry key edits, auditing, physical security, and third party tools. An additional step to this layered approach to security is modification of the permissions on the systems registry.

Following normal best practices, verify all these procedures in a test environment prior to implementation on any production systems. Back-up all registry keys and update the ERD disk prior to starting these changes. Do not undertake this exercise unless you are comfortable working in REGEDT32, Microsoft Security Console and have a working knowledge of the registry.

## Step 1: Ensure remote access to the registry is restricted

Although this is not a 'permissions of the registry' issue – it is too important as a 'permissions to the registry' issue to leave out or ignore.

- Δ Run *Regedt32*
- Δ Select *HKEY_LOCAL_MACHINE* in the local machine window
- Δ Drill down the *\System\CurrentControlSet\Control\SecurePipeServers* path
- Δ Create the *winreg* key if it is not present by,
- Δ Highlighting the *SecurePipeServers* key
- Δ Select **Add KEY** – from the **EDIT** menu
- Δ Enter "*winreg*" in the **Key Name:** field
- Δ Leave the **Class:** field blank
- Δ Click **OK** to close the **Add Key** window
- Δ Highlight the *winreg* key
- Δ Select **Add Value** – from the **Edit** menu
- Δ Enter "*RestrictGuestAccess*" for **Value Name:**
- Δ Select REG_DWORD from the **Data Type:** drop down list
- Δ Click **OK**
- Δ Enter *"1"* for the **Data:** value in the DWORD Editor
- Δ Click **OK**
- Δ Drill down the *\System\CurrentControlSet\Control\LSA* path
- Δ Highlight the *LSA* key
- Δ Select **Add Value** – from the **EDIT** menu
- Δ Enter "`RestrictAnonymous`" for Value Name
- Δ Select REG_DWORD from the **Data Type:** drop down list
- Δ Click **OK**
- Δ Enter "*1*" for the **Data:** value in the DWORD Editor
- Δ Click **OK**

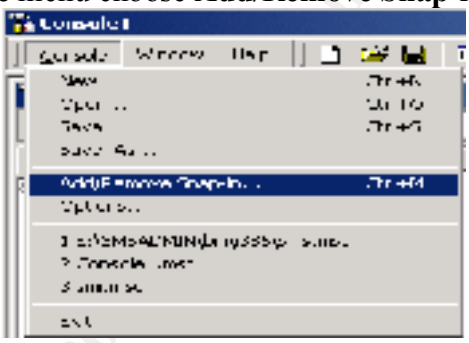
## Step 2: Security Configuration Manager (SCM)

The SCM was included on the Windows NT Service Pack 4 CD-Rom or may be downloaded from Microsoft's FTP server at the following address: ftp://ftp.microsoft.com/bussys/winnt/winnt-public/tools/scm.

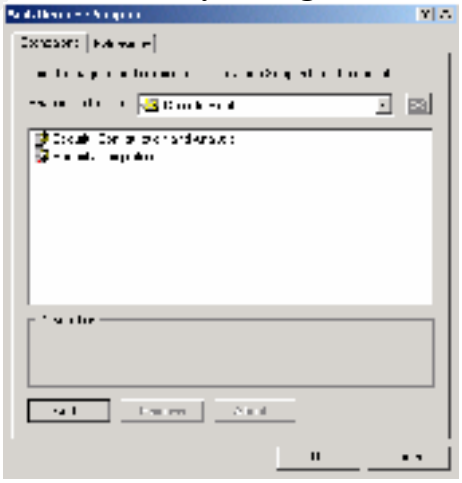
To install SCM – from a command prompt or from Windows NT Explorer – run the self-extracting file *scesp4i.exe*. To install both the GUI and command line tools, run *mssce.exe*. *Note – SCM is part of the Windows 2000 install. The command line tool allows for analysis of individual security areas as opposed to the entire configuration file. Additionally the results may be directed to a file for later review. Distributed system management tools may also use the command line tool to apply the configuration to remote or multiple systems.

To add SCM to the Microsoft Management Console (MMC) –

- Δ Run the MMC (*mmc.exe*)
- Δ From the **Console** menu choose **Add/Remove Snap-in**



- Δ Click **Add**
- Δ Select **Security Configuration Manager** (Windows 2000 users will add **Security Templates** and **Security Configuration and Analysis**)



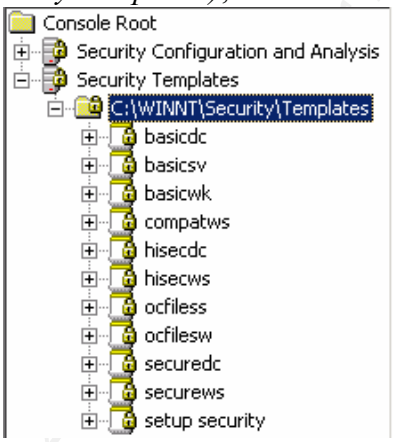
- Δ Click **OK**
- Δ Click **OK** again

**Note *** The SCM includes a set of pre-packaged configuration files. These files are located in *%SystemRoot%\Security\Templates*. These templates were designed for the three types of windows systems – workstation (wk), server (sv) and domain controller (dc), with three levels of available security – default (basic), compatible (comp) and secure (secur).

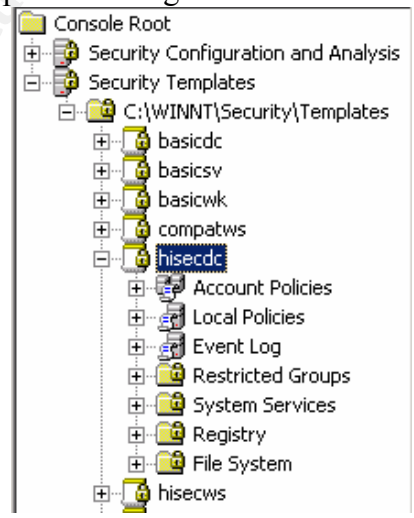
## Step 3: Edit the configuration file

The security and settings of any of the templates may be modified. To modify a configuration file these steps should be taken.

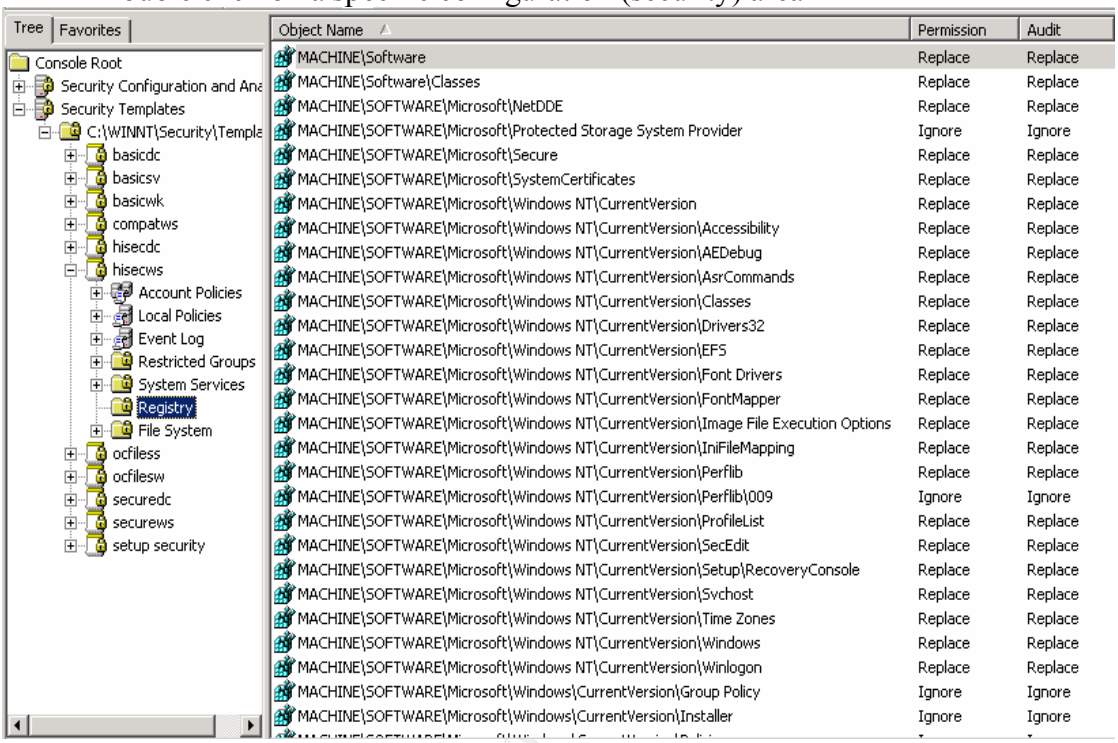
- Δ Within the MMC – double click on the **Security Configuration Manager** (Windows 2000 – **Security Templates**) node in the left pane
- Δ Double click the **Configurations** node (not required in Windows 2000)
- Δ Double click on the default configuration file directory (*%SystemRoot%\Security\Templates)*, the list of available files is revealed




- Δ Double click on a specific configuration file



Δ Double click on a specific configuration (security) area




Δ Double click on the specific security object in the right pane to modify

Δ To modify the security setting – right click the object and choose **Security**


Δ Customize all settings required by your environment

Δ Delete all extra settings not required by your environment (this step will increase system performance in applying the setting – but not increase the security of the system)

Δ Save the customized configuration file by right clicking on the file and choosing **Save As**

## Step 4: Recommended edits

All registry keys not listed are expected to maintain the inherited permissions of their parent key. Keys with "Ignore" are excluded from SCM configuration and retain their original permissions.

HKEY_CLASSES_ROOT\

| | | |
|---|---|---|
| | Administrators | Full Control |
| Key and subkeys | Creator/Owner | Full Control |
| * Alias to HKLM\SOFTWARE\Classes | System | Full Control |
| Contains file associations and Common Object Model (COM) associations | Authenticated Users | Read, Write, Execute |

HKEY_CLASSES_ROOT\.hlp

| | | |
|---|---|---|
| | Administrators | Full Control |
| Key | System | Full Control |
| Contains help file associations | Authenticated Users | Read, Execute |

HKEY_CLASSES_ROOT\helpfile

| | | |
|---|---|---|
| | Administrators | Full Control |
| Key | System | Full Control |
| Contains winhelp32 information | Authenticated Users | Read, Execute |

HKEY_LOCAL_MACHINE\HARDWARE

| | | |
|---|---|---|
| | Administrators | Full Control |
| Key | Creator/Owner | Full Control |
| Contains data about the physical configuration | System | Full Control |
| of the machine | Authenticated Users | Read, Write, Execute, Delete |

HKEY_LOCAL_MACHINE\SOFTWARE

| | | |
|---|---|---|
| | Administrators | Full Control |
| Key | Creator/Owner | Full Control |
| Contains data about the software installed | System | Full Control |
| of the machine | Authenticated Users | Read, Write, Execute, Delete |

HKEY_LOCAL_MACHINE\SOFTWARE\Classes IGNORE

Key and subkeys Contains file associations and Common Object Model (COM) associations

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography

| | | |
|---|---|---|
| Key and subkeys | Administrators | Full Control |
| Contains management for CryptoAPI | System | Full Control |
| | Authenticated Users | Read, Execute |

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NetDDE

| | | |
|---|---|---|
| Keys and subkeys | Administrators | Full Control |
| Contains settings for Network Dynamic Data Exchange, which is a protocol that allows Applications to exchange data | System | Full Control |

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Ole

| | | |
|---|---|---|
| Key and subkeys | Administrators | Full Control |
| Contains configuration for Object Linking | System | Full Control |
| and Embedding (OLE) | Authenticated Users | Read, Execute |

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\OS/2 Subsystems for NT

| | | |
|---|---|---|
| Key and subkeys | Administrators | Full Control |
| Contains support for OS/2 standards | Creator/Owner | Full Control |
| * Best practice is for this key to be deleted | System | Full Control |
| | Authenticated Users | Read, Execute |

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Protected Storage System Provider

| | |
|---|---|
| Key and subkeys | IGNORE |
| Used to protect user data – Inaccessible | |

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Rpc

| | | |
|---|---|---|
| Key and subkeys | Administrators | Full Control |
| Contains configuration for Remote Procedure | System | Full Control |
| Call (RPC) | Authenticated Users | Read, Execute |

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Secure

| | | |
|---|---|---|
| Key and subkeys | Administrators | Full Control |
| Contains Microsoft application configuration | Creator/Owner | Full Control |
| data that should only be changed by an | System | Full Control |
| administrator | Authenticated Users | Read, Execute |

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows

| | | |
|---|---|---|
| Key and subkeys | Administrators | Full Control |
| Contains the Win32 subsystem parameters | Creator/Owner | Full Control |
| | System | Full Control |
| | Authenticated Users | Read, Write, Execute |

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

| | | |
|---|---|---|
| Key and subkeys | Administrators | Full Control |
| Contains names of executables to be run | System | Full Control |
| each time the system is started | Authenticated Users | Read, Execute |

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

| | | |
|---|---|---|
| Key and subkeys | Administrators | Full Control |
| Contains names of programs to be run | System | Full Control |
| the first time a user ever logs in | Authenticated Users | Read, Execute |

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx

| | | |
|---|---|---|
| Key and subkeys | Administrators | Full Control |
| Contains setup information for system components | System | Full Control |
| and Internet Explorer | Authenticated Users | Read, Execute |

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Shell Extensions

| | | |
|---|---|---|
| Key and subkeys | Administrators | Full Control |
| Contains all shell extension settings to extend the Windows NT interface | Creator/Owner | Full Control |
| | System | Full Control |
| | Authenticated Users | Read, Execute |

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall

| | | |
|---|---|---|
| Key and subkeys | Administrators | Full Control |
| Contains uninstall strings for all applications that can be removed by Add/Remove Programs | Creator/Owner | Full Control |
| | System | Full Control |
| | Authenticated Users | Read, Execute |

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT

| | | |
|---|---|---|
| Key and subkeys | Administrators | Full Control |
| Contains parameters used by the Windows NT operating system | Creator/Owner | Full Control |
| | System | Full Control |
| | Authenticated Users | Read, Execute |

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AEDebug

| | | |
|---|---|---|
| Key and subkeys | Administrators | Full Control |
| Contains settings for Dr. Watson or other application debuggers | System | Full Control |
| | Authenticated Users | Read, Execute |

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Compaibility

| | | |
|---|---|---|
| Key and subkeys | Administrators | Full Control |
| Contains data for legacy applications not completely compatible with Windows NT | Creator/Owner | Full Control |
| | System | Full Control |
| | Authenticated Users | Read, Write, Execute |

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Font Drivers

| | | |
|---|---|---|
| Key and subkeys | Administrators | Full Control |
| Contains drivers to display fonts | System | Full Control |
| | Authenticated Users | Read, Execute |

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Font Mapper

| | | |
|---|---|---|
| Key and subkeys | Administrators | Full Control |
| Contains settings for mappings of unavailable fonts To existing fonts | System | Full Control |
| | Authenticated Users | Read, Execute |

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options

| | | |
|---|---|---|
| Key and subkeys | Administrators | Full Control |
| Contains parameters for viewing images | System | Full Control |
| | Authenticated Users | Read, Execute |

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\IniFileMappings

| | | |
|---|---|---|
| Key and subkeys | Administrators | Full Control |
| Contains mappings for 16-bit Windows | System | Full Control |
| application initialization files | Authenticated Users | Read, Execute |

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib

| | | |
|---|---|---|
| Key and subkeys | Administrators | Full Control |
| Contains parameters for the performance library | System | Full Control |
| which collects data for performance monitor | Authenticated Users | Read, Execute |

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib\009

| | |
|---|---|
| Key and subkeys | IGNORE |
| Contains performance names and descriptions | |

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones

| | | |
|---|---|---|
| Key and subkeys | Administrators | Full Control |
| Contains time zone settings | System | Full Control |
| | Authenticated Users | Read, Execute |

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

| | | |
|---|---|---|
| Key and subkeys | Administrators | Full Control |
| Contains logon sequence controls | System | Full Control |
| | Authenticated Users | Read, Execute |

HKEY_LOCAL_MACHINE\SOFTWARE\Program Groups

| | | |
|---|---|---|
| Key and subkeys | Administrators | Full Control |
| Contains information about former program groups | Creator/Owner | Full Control |
| if a pre-NT 4.0 operating system has been converted | System | Full Control |
| | Authenticated Users | Read, Execute |

HKEY_LOCAL_MACHINE\SOFTWARE\Secure

| | | |
|---|---|---|
| Key and subkeys | Administrators | Full Control |
| Contains application configuration | Creator/Owner | Full Control |
| data that should only be changed by an | System | Full Control |
| administrator | Authenticated Users | Read, Execute |

HKEY_LOCAL_MACHINE\SOFTWARE\Windows 3.1 Migration Status

| | | |
|---|---|---|
| Key and subkeys | Administrators | Full Control |
| Contains data if the system has been upgraded from | Creator/Owner | Full Control |
| Windows 3.1 to Windows NT | System | Full Control |
| | Authenticated Users | Read, Execute |

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg

| | | |
|---|---|---|
| Key and subkeys | Administrators | Full Control |
| The security permissions assigned to this key define which users have remote access to the registry. Default Windows NT Workstation installation does not define this key and does not restrict remote access to the registry. Windows NT Server permits only administrators' remote access to most of the registry. It is highly recommended that only administrators have remote access to the registry. | System | Full Control |

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Shares

| | | |
|---|---|---|
| Key and subkeys | Administrators | Full Control |
| Contains settings for the local system shares | Creator/Owner | Full Control |
| | System | Full Control |
| | Authenticated Users | Read, Execute |

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Schedule

| | | |
|---|---|---|
| Key and subkeys | Administrators | Full Control |
| Contains settings for the scheduler service | Creator/Owner | Full Control |
| | System | Full Control |
| | Authenticated Users | Read, Execute |

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\UPS

| | | |
|---|---|---|
| Key and subkeys | Administrators | Full Control |
| Contains information on the Uninterruptible Power | Creator/Owner | Full Control |
| Supply if installed | System | Full Control |
| | Authenticated Users | Read, Execute |

HKEY_USERS\.DEFAULT

| | | |
|---|---|---|
| Key and subkeys | Administrators | Full Control |
| Profile that is used while the Windows NT | System | Full Control |
| CTL-ALT-DEL Logon Message is displayed | Authenticated Users | Read, Execute |

HKEY_USERS\.DEFAULT\Software\Microsoft\NetDDE

| | | |
|---|---|---|
| Key and subkeys | Administrators | Full Control |
| Settings for Network Dynamic Data Exchange, which is a protocol that allows applications to exchange data | System | Full Control |

HKEY_USERS\.DEFAULT\Software\Microsoft\Protected Storage Systems Provider

| | |
|---|---|
| Key and subkeys | IGNORE |
| Used to protect user data –inaccessible | |

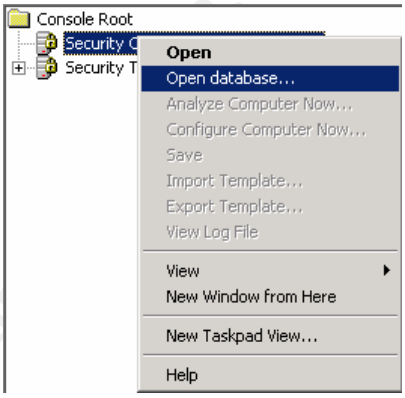
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows|CurrentVersion\Policies

| | | |
|---|---|---|
| Key and subkeys | Administrators | Full Control |
| Used to manage Recreational Software Advisory | Creator/Owner | Full Control |
| Council (RASC) ratings | System | Full Control |
| | Authenticated Users | Read, Execute |

## Step 5: Assigning the configuration to a database

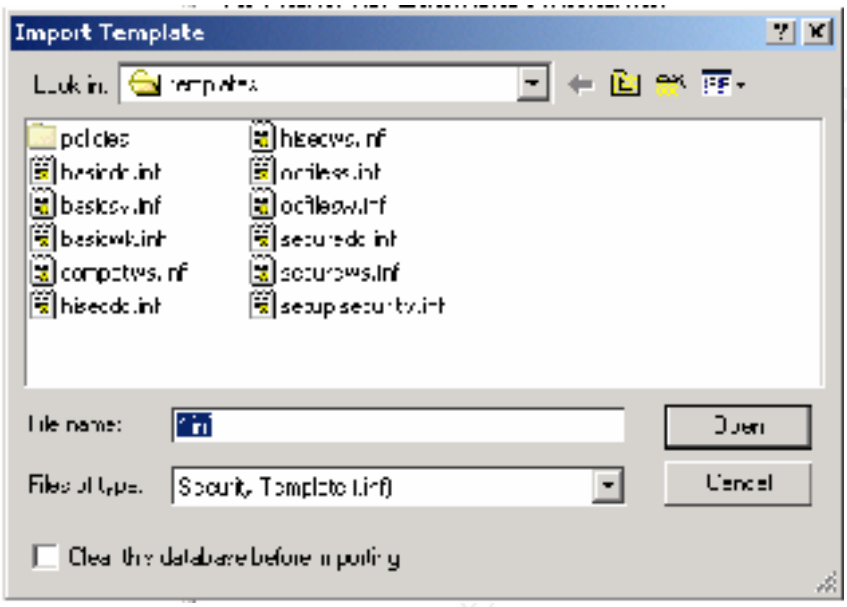
After completing the creation of your ".inf" file, you can analysis and configure the system. The creation of the ".inf" file can be done from any Windows NT or Windows 2000 system, and applied to other systems as needed. The security analysis and configuration may be performed from the GUI or from a command line. The command line allows you to create a batch file and perform these actions on multiple systems or at a predetermined interval using the scheduler service or a third-party tool. *Always remember to completely test the configuration file prior to applying it to a production box as a loss in performance and/or functionality may result.

- Δ The SCM uses a database to store configurations for both the analysis and application of the configuration. A best practice is to create a new database for each analysis and configuration. Import operations can append to or overwrite the database information. Appending is the default setting, but may cause confusion and/or unwanted combining of configurations. Check the "Overwrite existing configuration in database" to avoid this problem.
- Δ To open an existing or new database in the SCM GUI. Right click on the **Database** node
- Δ Select **Open Database**




- Δ Enter the name of the database you wish to create – or the name of an existing database.
- Δ Click **Open**
- Δ If a new database name was entered the system will automatically prompt you to enter the configuration file to import.
- Δ If you use an existing database – right click on the **Database** node – choose **Import Configuration**

Δ In the **Select Configuration to Import** dialog box – choose the ".inf" file you just created.



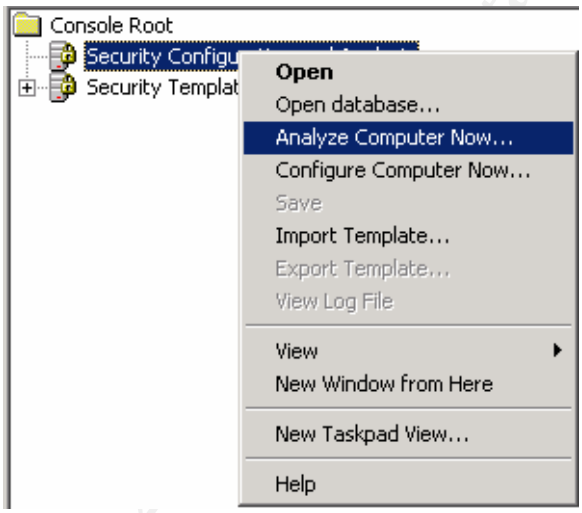

Δ Check the **Overwrite existing configuration in database** box to remove all previous stetting stored in the database. (Windows 2000 users – **Clear this database before importing)**


Δ Click **Open**.

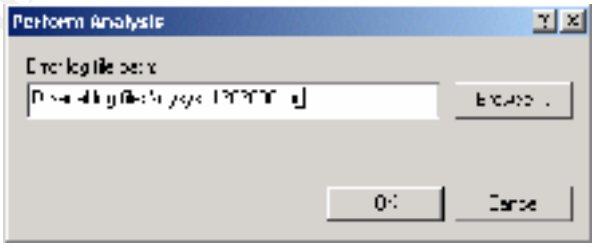
## Step 6: Performing the analysis

The analysis is actually run against the database, which is using the configuration file(s) ".inf" that have been imported. The current system settings are compared to the configuration settings in the configuration files and the results are stored back into the database. Both the current settings and the configuration settings are then displayed side by side and additional modifications to the configuration setting may be made and saved back to the ".inf" file.

- Δ From the SCM in MMC right click on the **Database** node
- Δ Select **Analyze System Now**




- Δ Enter an error log file path into the **Perform Analysis** dialog box. The log information is appended to the specified log file. You must specify a new file name if you want a new or separate log to be created.




- Δ Click **OK**
- Δ Examine and modify the settings as needed.

## Step 6a: Performing the Analysis from the command line

To perform these same actions from the command line, use the following syntax. This syntax may be used in a batch file.

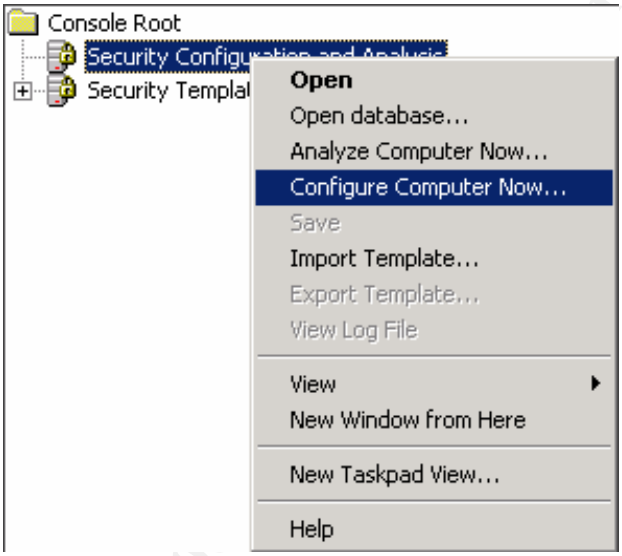
*Secedit /analyze [/cfg* filename*] [/db* filename*] [/log* logpath*] /verbose [/quiet] [/overwrite] [>> results_file]*

**/cfg** --- Path to the .inf file that will be appended to the database prior to the analysis
**/db** --- Path the database that SCE will perform the analysis against. If this variable is not set than the last database used in analysis or configuration is used. The system default database is *%systemroot%\security\database\secedit.sdb*.
**/log** --- Path to the log file for the process. If this file is not specified, the progress information will be output to the console.
**/verbose** --- Specify detailed progress information.
**/quiet** --- Suppress screen and log output.
**/overwrite** --- This will overwrite the named database with the configuration file information. This is a recommended switch to avoid unwanted combinations of configurations.
**>> results_file** --- This is the name and path of the file you wish to contain the results of the analysis. This file allows you to analysis at any time and review the results later.

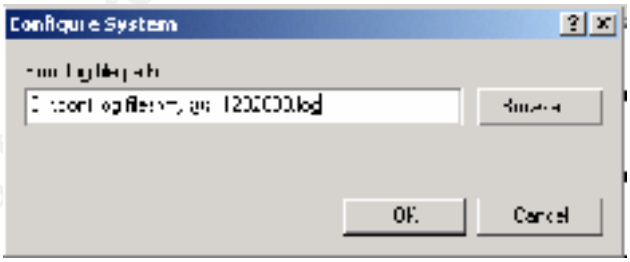
## Step 7: Configuring the system

Some errors may result during the configuration if specific registry keys do not exist on the system, but are included in the .inf file. This is a normal condition due to the generic nature of the .inf files that were included in the SCM, and should cause no alarm.

- From the SCM GUI – right click on the **Database** node
- Select **Configure Now**




- Enter the error log file path into the **Configure System** dialog box




- Click **OK**
- Reboot the system.

## Step 7a: Configuring the system using the command line

To configure a system from the command line – use the following syntax

*Secedit /configure [/cfg* filename*] [/db* filename*] [/log* logpath*] /verbose [/quiet] [/overwrite] [areas* Areas*]*

**/cfg** --- Path to the .inf file that will be appended to the database prior to the analysis
**/db** --- Path the database that SCE will perform the analysis against. If this variable is not set than the last database used in analysis or configuration is used. The system default database is *%systemroot%\security\database\secedit.sdb*.
**/log** --- Path to the log file for the process. If this file is not specified, the progress information will be output to the console.
**/verbose** --- Specify detailed progress information.
**/quiet** --- Suppress screen and log output.
**/overwrite** --- This will overwrite the named database with the configuration file information. This is a recommended switch to avoid unwanted combinations of configurations.
**/areas ---** This will apply specific areas of the .inf file – for registry permissions use "**REGKEYS**" – if this switch is not used then all areas of the .inf will be applied.

## Step 8: Insure configurations remain constant

Once all settings have been made and applied – each system should be checked periodically to ensure the current system configuration has not changed. This can be scripted thru batch file analysis and reviewed either manually or thru automated means. This provides an additional means to monitor for intrusions based on both the analysis of the security configuration and by use of auditing.

## References:

*Guide to Securing Microsoft Windows NT Networks*
National Security Agency : Report number C4-008R-99
*Guide to Windows NT Security*
Charles B Rutstein – McGraw Hill – ISBN 0-07-057833-8
*Windows NT Security Handbook*
Tom Sheldon – Osborne McGraw Hill – ISBN 0-07-882240-8
*Windows 2000 Security*
Roberta Bragg – New Riders – ISBN 0-7357-0991-2
*Microsoft Windows 2000 Server Administrator's Companion*
Russel Crawford – Microsoft press – ISBN 1-57231-891-8
*Windows NT System Administration*
Aeleen Frisch – O'Reilly – ISBN 1-56592-274-3
*Microsoft TechNet*
Multiple months and Knowledge Base articles
*Securing Windows NT Step-by-Step*
Jennifer Kolde, Jason Fossen – SANS Institute 2000

Other GIAC Research papers to help shed light on this same topic or tools:

*Securing Windows NT*
Andrew Kjell Nielsen
*IT Services security plan –*
*GIAC NT*
Don Michelli
*Securing Microsoft IIS 5 using Windows 2000 Internet Server Security Configuration Tool*
George M. Garner Jr.
*Limiting Anonymous Logon/Network Access to Named Pipes and Shares*
John W. Albright

Last Updated: July 27th, 2017

# Upcoming Training


| | | | |
|---|---|---|---|
| SANS Virginia Beach 2017 | Virginia Beach, VA | Aug 21, 2017 - Sep 01, 2017 | Live Event |
| SANS Network Security 2017 | Las Vegas, NV | Sep 10, 2017 - Sep 17, 2017 | Live Event |
| SANS vLive - SEC505: Securing Windows and PowerShell Automation | SEC505 - 201709, | Sep 18, 2017 - Nov 13, 2017 | vLive |
| Secure DevOps Summit & Training | Denver, CO | Oct 10, 2017 - Oct 17, 2017 | Live Event |
| SANS San Francisco Winter 2017 | San Francisco, CA | Nov 27, 2017 - Dec 02, 2017 | Live Event |
| San Francisco Winter 2017 - SEC505: Securing Windows and PowerShell Automation | San Francisco, CA | Nov 27, 2017 - Dec 02, 2017 | vLive |
| SANS Cyber Defense Initiative 2017 | Washington, DC | Dec 12, 2017 - Dec 19, 2017 | Live Event |
| SANS Southern California- Anaheim 2018 | Anaheim, CA | Feb 12, 2018 - Feb 17, 2018 | Live Event |
| SANS OnDemand | Online | Anytime | Self Paced |
| SANS SelfStudy | Books & MP3s Only | Anytime | Self Paced |