Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Step-By-Step Guide
To
Securing Windows 2000 Server
Using the Security Configuration
&
Analysis Tool

Prepared for:

SANS GIAC GCNT Certification
Jason Morris
March 2001

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

© SANS Institute 2000 - 2002, Author retains full rights.

This page intentionally left blank.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

TABLE OF CONTENTS

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

TABLE OF FIGURES

©SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

1. INTRODUCTION

With the release of Windows 2000 Server there really is no excuse for not having a reasonably secure system. In fact, Windows 2000 is much more secure out of the box than Windows NT 4.0 was. This is especially true if Windows 2000 is clean-installed onto an NTFS partition. The default security settings are applied during installation. A template file, similar in format to the one we will create later on in this guide, is used to make these changes. These default templates are:

- %windir%\inf\defltwk.inf – for configuring workstations
- %windir%\inf\defltsv.inf – for configuring servers
- %windir%\inf\defltdc.inf – for configuring domain controllers.[1]

There are tools now available which come with the operating system that are very nice, relatively easy to use, and powerful as well. These tools allow you to make changes to the configuration of the system thereby increasing its security. There are a number of ways to make these configuration changes. They can be made manually, by hand editing the registry, setting permissions manually, or setting account policies and user rights manually. They can also be made using Group Policy. The tool outlined by this paper however is the Microsoft Management Console using the Security Configuration and Analysis snap-in.

Though the bulk of this paper deals with using the MMC and the Security Configuration and Analysis snap-in to secure Windows 2000 server there are several other things that are critical to the security of your system. These will be discussed briefly for completeness.

A major goal of this paper is to create a security configuration template that meets the security requirements as defined in your corporate security policy. Once created this template can then be taken to any other similar system that requires security configuration. The template can also be modified later if you decide that something was left out or something new needs to be included in it.

We will not attempt to go into each of the explicit configuration changes made by the template described in this paper. Space does not allow for complete coverage of these settings and there are numerous other resources that do cover these configuration changes. Most of the changes made by the template file are documented elsewhere. This paper is concerned more with how to create the template than what the template changes on the system.

This paper has various sections in it, which contain some background information about the topic being covered in the section as well as explanatory text interspersed throughout the section. The sections also have a **Steps To Follow** part to them, which contain the actual steps that someone would follow to complete the procedures.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

2. CREATING AN EMERGENCY REPAIR DISK

We will start out by creating an emergency repair disk. Though maybe not a critical component of system security, creating and using emergency repair disks is just plain smart system administration. Also, since the changes being made by the steps in this paper radically alter the system and the registry, creating an ERD makes good sense.

The procedure used to create emergency repair disks has changed with the release of Windows 2000. With previous versions of Windows NT the rdisk command was used to create them. In Windows 2000 the **NTBACKUP** command is used.

Steps To Follow

1. Have a floppy ready. From **Start** | **Run** enter **ntbackup** and click **OK**. In the **Welcome to the Windows 2000 Backup and Recovery Tools** window, click on the **Emergency Repair Disk** button and follow the instructions.

Figure 1 - Emergency Repair Disk Creation Window

Store the ERD in a safe place and update as needed when the system configuration changes.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

3. CONFIGURE ALL DRIVES AS NTFS

A big part of security as it relates to Windows 2000 as well as Windows NT is enabled through NTFS file and folder permissions. If security is a concern in your environment you will not want to use FAT formatted partitions. NTFS v.5, which is the new version of the NTFS file system, brings some nice new features to the proverbial table. Windows 2000 NTFS formatted drives support Encrypting File System (EFS). This allows you to encrypt files on your hard drive. NTFS v.5 also gives you greater flexibility in managing your disk drives.

Many of the configuration changes that will be made with the configuration template, which will be created and applied later on, will fail if the drive(s) are not formatted using NTFS.

Steps To Follow

1. Right click on the **My Computer** desktop icon and select **Manage**. In the **Computer Management** window under **Storage**, select **Disk Management**. Review the disk partition types to check formatting.

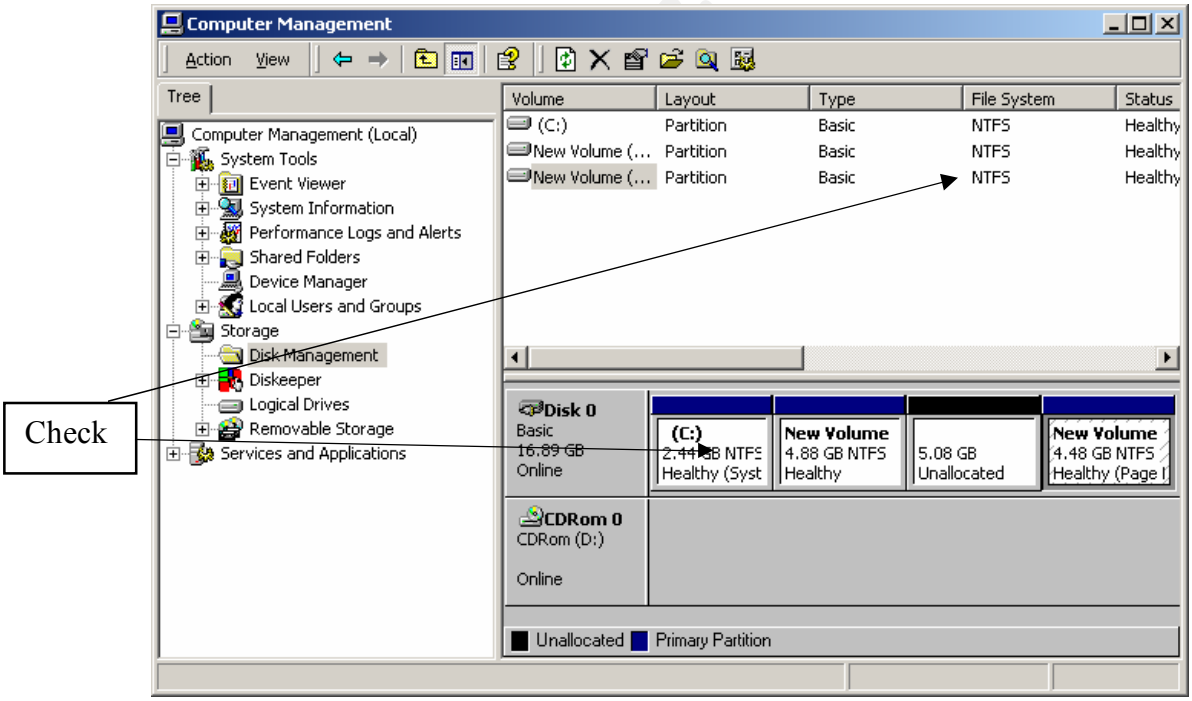

Figure 2 - Checking NTFS Formatting

If you find drives that are not formatted as NTFS in the Disk Management window it is not a good idea to format them here. It can be done, however, loss of data will result. If there is nothing on the partition, then it is ok to format it here. If the drive(s) have data on them that needs to be kept, use the **convert** command. This

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

will allow you to change the format of a drive from FAT to NTFS without the normal resultant loss of data. It would be a good idea to have a good backup of the drive in case something goes wrong. From a command line the syntax would look something like: **convert d: /fs:ntfs**, where d: is the drive you would like to convert to NTFS. Use the /v switch for verbose mode if you would like more detail.

4. APPLICATION OF SERVICE PACKS

Essential to achieving and maintaining a secure system is the application of service packs. As bugs or vulnerabilities are discovered in the operating system Microsoft releases hotfixes to correct them. These are bundled into the latest service pack. Since many of them pertain to system security, application is necessary to keep your system's security up to date.

Steps To Follow

1. Right click on the **My Computer** icon on the desktop and select **Properties** from the context menu. Verify that the system is running the latest service pack. If not, download it from Microsoft's web site and follow the instructions that come with the service pack to install it.

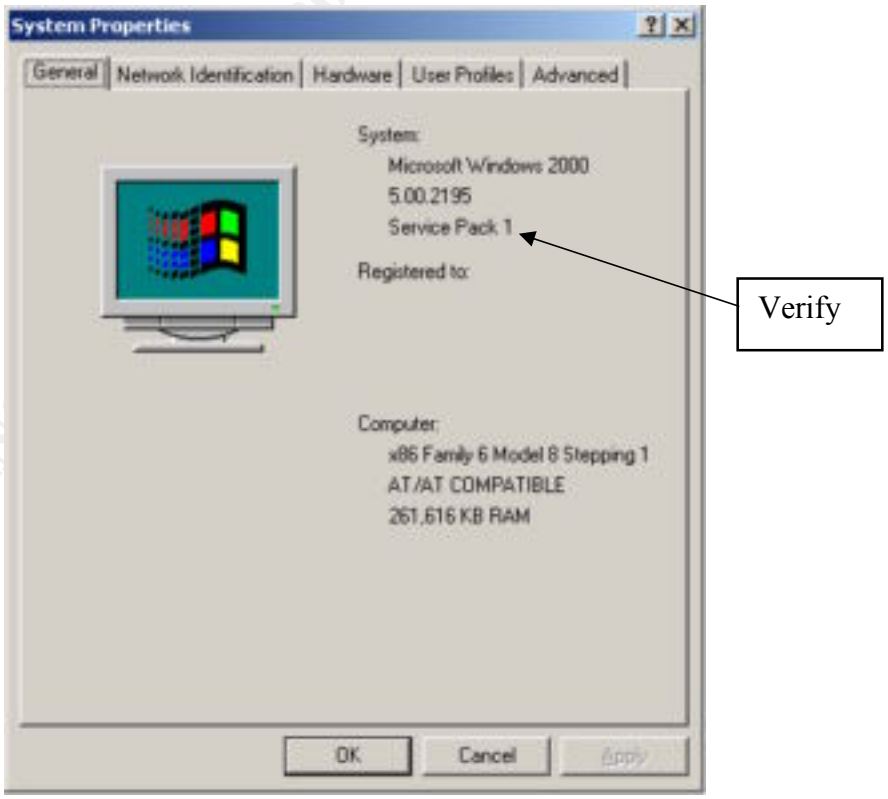

Figure 3 - Service Pack Verification

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

5. INSTALLATION OF WINDOWS 2000 HIGH ENCRYPTION PACK

Application of the Windows 2000 High Encryption Pack is necessary to bring the system up to 128-bit encryption. This affects a number of areas. A few of these are: upgrading Internet Explorer to use 128-bit SSL, it allows you to use 128-bit encryption with the Terminal Services Remote Desktop Protocol (RDP), and it also allows the use of 128-bit encryption for remote access using RRAS.

Steps To Follow

1. Download the compressed High Encryption Pack file from the Microsoft web site (Encpack_Win2000Admin_EN.exe).

2. Expand this file. Then double click the file **encpack.exe**. From the **Microsoft Windows 2000 High Encryption (128-bit) Capability** dialog box, click **Yes**. Click **Yes** on the **Licensing Agreement Acceptance** window. Click **Yes** to restart the computer.

3. Once you have rebooted and logged back on, use Explorer and navigate to %systemroot%\system32 (i.e. c:\winnt\system32). Right click on the **schannel.dll** file and select **Properties**. Select the **Version** tab and verify the settings on the following graphic. This is one way to verify that your system is using 128-bit encryption.

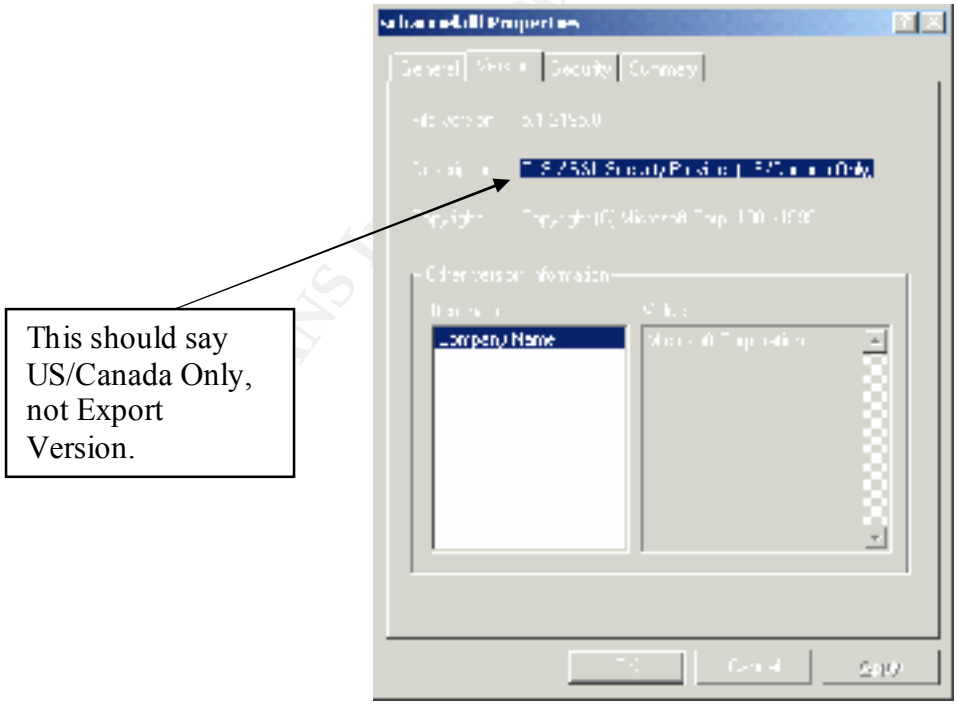

Figure 4 - Verification of 128-bit Encryption

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

6. CREATION OF THE SECURITY POLICY TEMPLATE

We now have a system that has a good foundation for building our security template on. We are ready to begin the real security configuration. The Microsoft Management Console is the tool we will now use to start our configuration. There are a number of pre-made security templates that come with Windows 2000. These are text files with a lot of changes in them, which are interpreted by the MMC and snap-in. These templates can be found in the **%systemroot%\security\templates** folder.

Template File Name	System Use
basicwk.inf	Default workstation
basicsv.inf	Default server
basicdc.inf	Default domain controller
compatws.inf	Compatible workstation or server
notssid.inf	Terminal Services backward compatibility
securews.inf	Secure workstation or server
hisecws.inf	Highly secure workstation or server
securedc.inf	Secure domain controller
hisecdc.inf	Highly secure domain controller

Table 1 – Some Default Template Files

Basic (basic*.inf)

The basic templates are used to back out the changes made by applying one of the more stringent templates. This will reapply the default security settings. The exception here is that of user rights. These will be unaffected so they will need to be corrected by hand. I would not really consider this a security template because it does not increase the security of the system.

Compatible (compatws.inf)

This template is used primarily to achieve backward compatibility for applications. The default security settings for Windows 2000 are stricter than they were for Windows NT 4.0, hence some users who are only members of the Users group may have some problems running certain applications. The Power Users group in Windows 2000 loosely corresponds to those of the Users group in Windows NT 4.0. This template eases some of the security settings for files, folders, and registry keys which are sometimes accessed by applications. This does not increase the security of the system so I don't consider this a security template.

Terminal Services (notssid.inf)

This template file allows older programs to run properly on a Windows 2000 server running Terminal Services. It accomplishes this by granting additional permissions to Terminal Services users. Once this template is applied the system has

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

the same default permissions as a standard Windows 2000 server that is running Terminal Services.[2]

Secure (secure*.inf)

This template sets numerous parameters like account and password policy, audit policy, and makes a number of registry changes. This template does not affect file, folder, and registry key permissions.

Highly Secure (hisec*.inf)

This group of templates is the most stringent of the default templates. This template makes all of the changes set by the Secure group of templates as well as setting permissions on file, folder, and registry keys.[3]

For the purposes of this paper we will be using the **hisecws.inf** template. It is the template to use if the system being configured is running the Windows 2000 Server or the Windows 2000 Professional operating systems.

Steps To Follow

1. Start with a machine that has a clean installation of Windows 2000 Server on it. The template that will be used for subsequent configurations will be created on this system.

2. Click **Start** | **Run**, type **mmc** and click **OK**. On the **Console** menu item select the **Add/Remove Snap-in…** menu item. Click **Add** on the **Add/Remove Snap-in** window. From the **Add Standalone Snap-in** window scroll down to **Security Configuration and Analysis**, highlight it and click **Add**. The window looks like the following graphic.

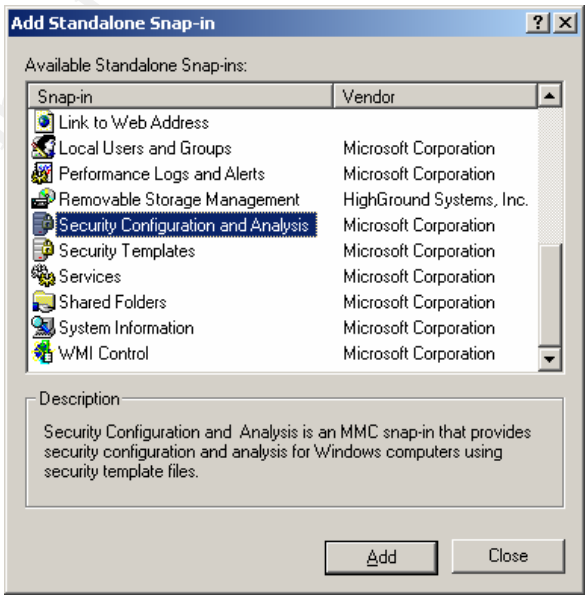

Figure 5 - Security Configuration & Analysis Snap-in

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

3. In the **Add Standalone Snap-in** window click **Close**. Click **OK** on the **Add/Remove Snap-in** window. Your screen should now look like the following graphic.

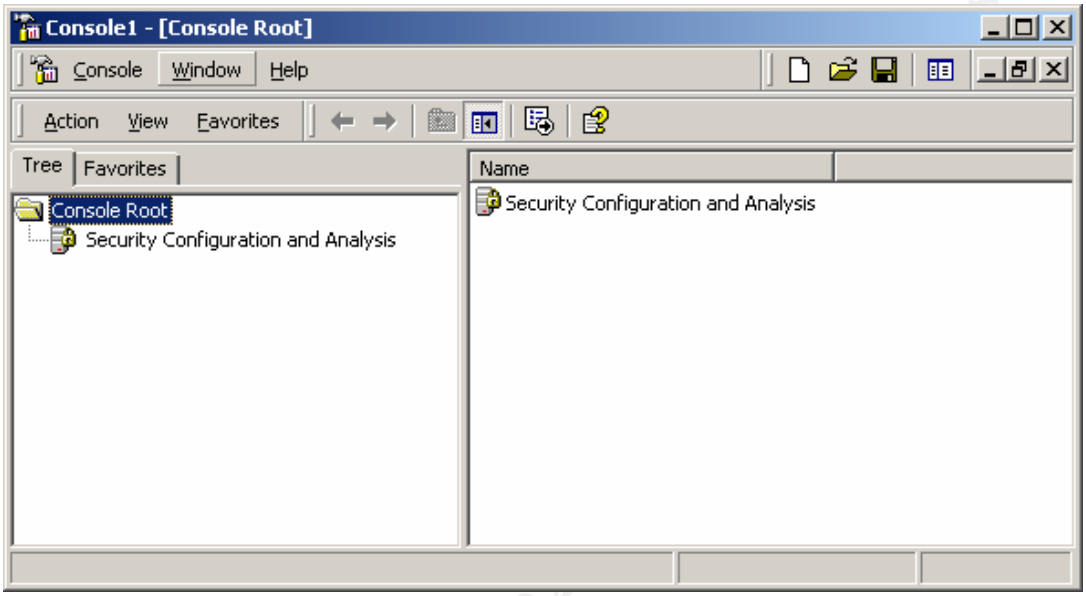

Figure 6 - MMC with Snap-in

4. We will now create a custom console for use in a script file we will create in Section 7. Click the **Console** menu item and click **Save**. In the **Save As** window in the **File name:** section enter an appropriate name (i.e. SecurityConfiguration_Analysis.msc). The **Save in:** section just needs to be a path where you can find the file when you need it later. Click **OK**.

5. Right click **Security Configuration and Analysis** and select **Open database…** from the menu. In the **Open database** window in the **File name:** section type in an appropriate name. This can be anything descriptive of your configuration (i.e. win2ksvrhisec.sdb). Click **Open**. In the **Import Template** window select the **hisecws.inf** file and click **Open**.

At this point if you did not want to make any changes to the preconfigured template you could go ahead and configure your system now based upon the parameters in the hisecws.inf template. **(We are not going to yet)** To do so you would right click Security Configuration and Analysis and select Configure Computer Now… At this point the assumption is that you would like to alter the default template in some way to more closely match your corporate security policy.

6. Right click **Security Configuration and Analysis** in the left pane. Select **Analyze Computer Now…** You can change the location of the log location in the **Perform Analysis** window to %windir%\security\logs if you like. The security subfolder under the %windir% directory is created by the system by

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

default. This is a good place to put files related to system configuration templates. This will make finding and reviewing them easier. It is also ok to accept the default in the **Perform Analysis** window and click **OK**. It is up to you. Wait while the system analyzes the current security configuration. When it is complete you can expand **Security Configuration and Analysis**. Your screen should look like the following graphic.

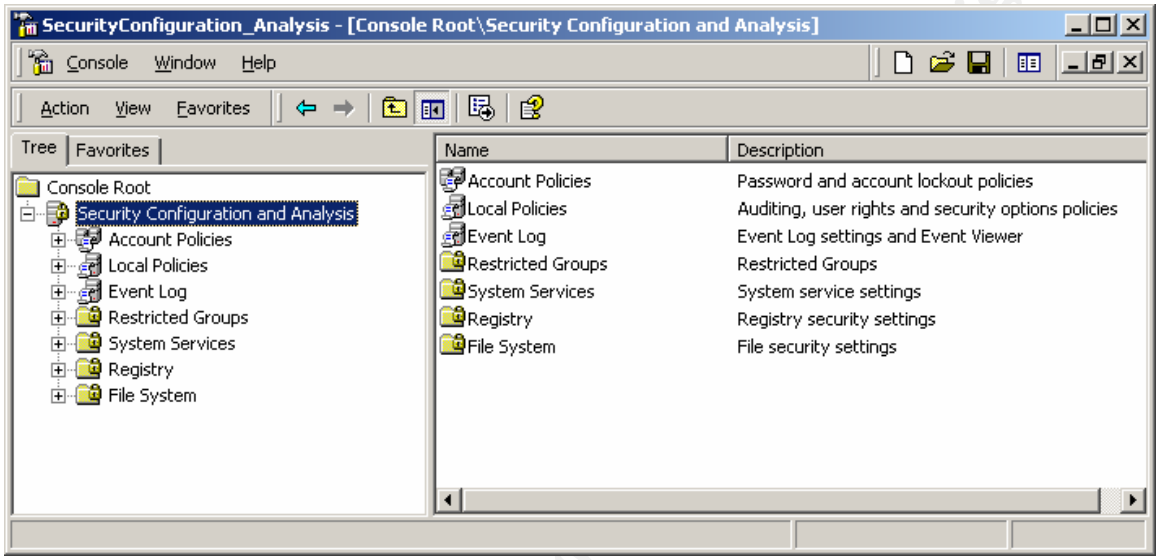

Figure 7 - After Analyzing the System

The current system configuration has been compared with that of the security configuration template, but no actual changes have been made. For some organizations these potential changes would be sufficient.

At this point you could look through the various settings to see the changes that would be made to the system and then configure the system using these settings. We will make some changes to the template to give an example of how it would be done. The system can then be configured and the template saved out so that it can be applied to any number of systems. This will give you very consistent results.

If you expand one of the sections like **Account Policies | Password Policy** in the right pane you will see some parameters that could be configured. The red circle with the white X in it indicates discrepancies between the template configuration and the current setting on the system. The circle with the green check mark in it indicates a match between the template and the system. The column in the right pane entitled **Database Setting** corresponds to the security template. The column entitled **Computer Setting** is the current setting of that attribute on the system itself. Please refer to the graphic below.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

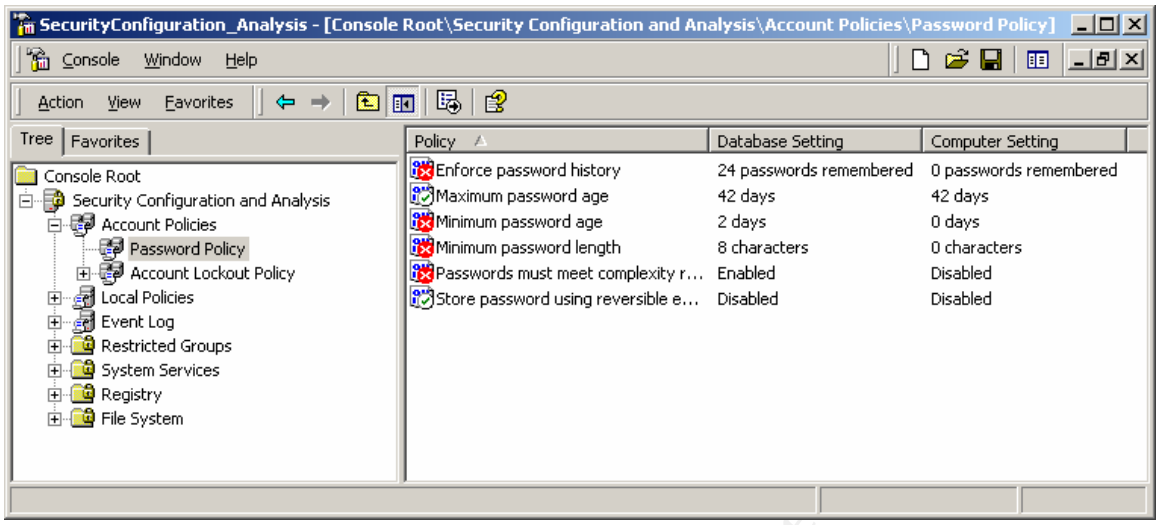

Figure 8 - Difference Between Database & Computer Settings

7. Let's assume that the **Enforce password history** value should be changed from the template value of 24 passwords remembered to 5 passwords remembered. Double click the **Enforce password history** entry. As an example change the value in **Keep password history** to **5**. The screen should resemble the graphic below. Click **OK**.

Figure 9 - Enforce Password History Setting Example

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

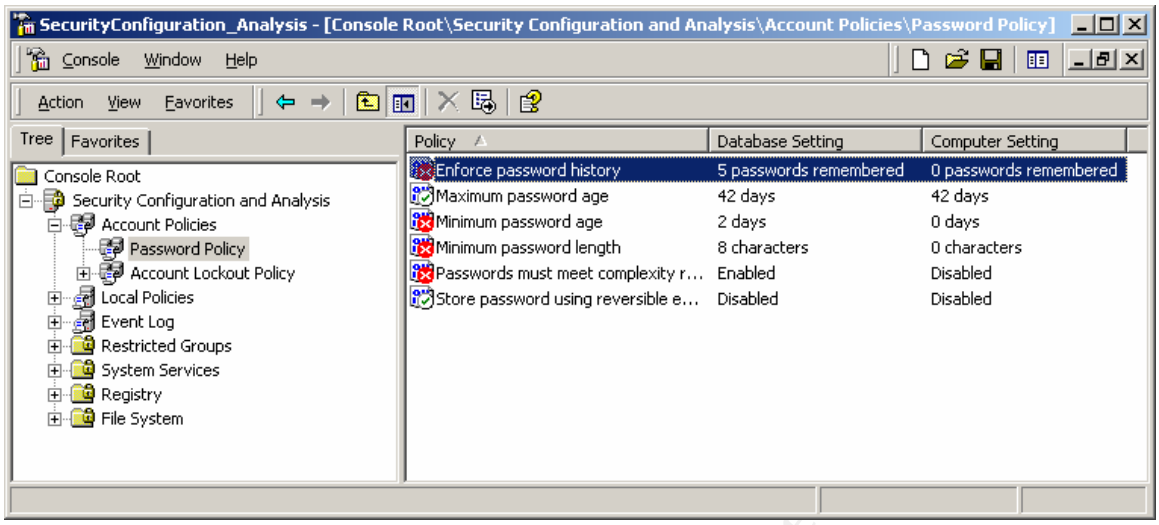

Figure 10 – Updated MMC Window With New Password Policy Value

Notice the new value entry in the Database Setting column in the above graphic.

8. Let's assume that we want to make an additional change for illustration purposes. If we expand **Local Policies | Security Options** we find a number of parameters that can be set. Find **Restrict CD-ROM access to locally logged-on user only** and double click it. Click the radio button next to **Enabled**. The screen should resemble the graphic below. Click **OK**.

Figure 11 – Restrict CD-ROM Access Example

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

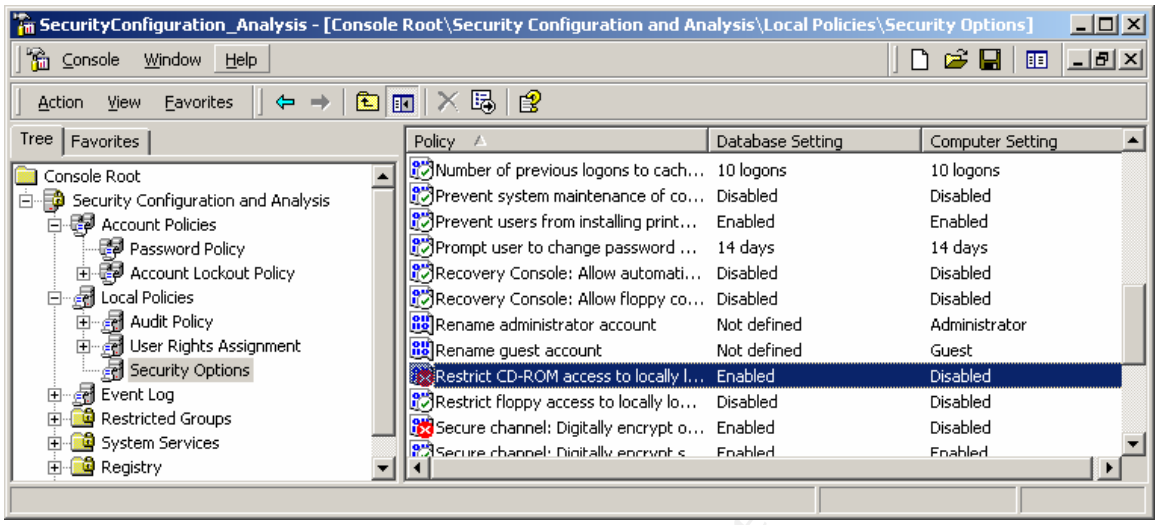

Figure 12 – Updated MMC Window With New Restrict CD-ROM Value

Notice the new value entry in the Database Setting column in the above graphic.

> **Note: You could follow similar steps to make any other changes that you feel are pertinent to your environment.**

Let's now assume that these are the only changes that need to be made.

> ***Important Note: See Section 7, Known Gotcha before proceeding with Step 9.***

We now need to save these changes out to a new template file that can then be used to configure this system or any others that need configuration.

9. Right click on **Security Configuration and Analysis** and click **Save**. Right click again on **Security Configuration and Analysis** and click **Export Template…** In the **Export Template To** window in the **File name:** section enter an appropriate and descriptive name (i.e. win2ksvrhisec.inf) and click **Save**.

10. Leave the Microsoft Management Console open to continue on with the steps in Section 8.

A new template that has all of the configuration changes that meet your corporate policy has now been created. The current system can now be configured using this template and the template is ready to be taken to other systems for their configuration. We will cover that in Section 8.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

7. KNOWN GOTCHA

There is a known gotcha with the template that we have configured in the previous steps. You might want to review this before proceeding to Section 8. This particular configuration setting is in the hisecws.inf template by default. Once you apply the template it changes the challenge/response authentication to NTLMv2. It looks like the following graphic.

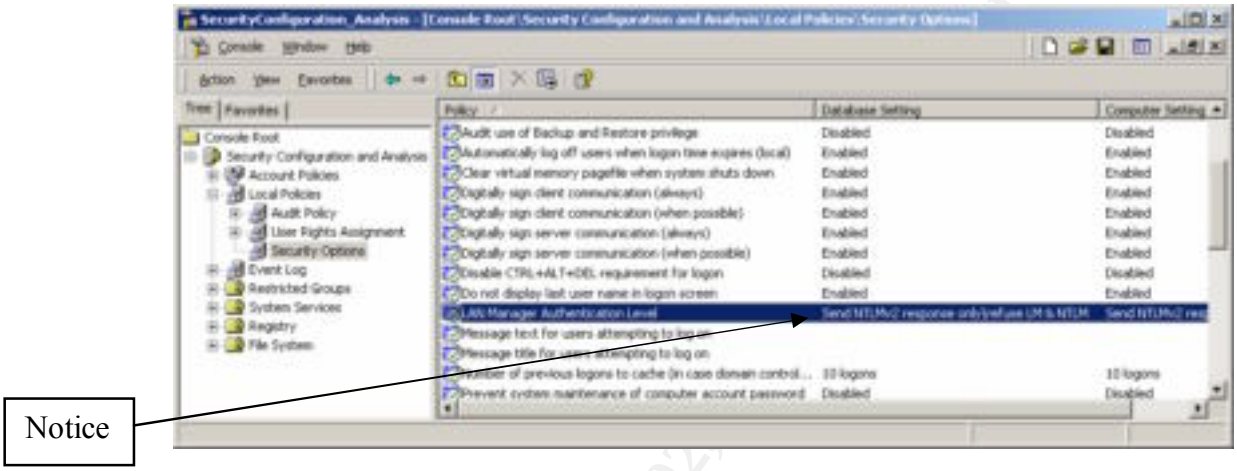

Figure 13 – Changed LAN Manager Authentication

NTLMv2 is much more secure than the other two authentication mechanisms, LM and NTLM.[4] However, there seem to be problems joining the Windows 2000 system to Windows NT 4.0 domains. If the primary domain controller you are trying to join is running at service pack 4 you will get the message in the following graphic.

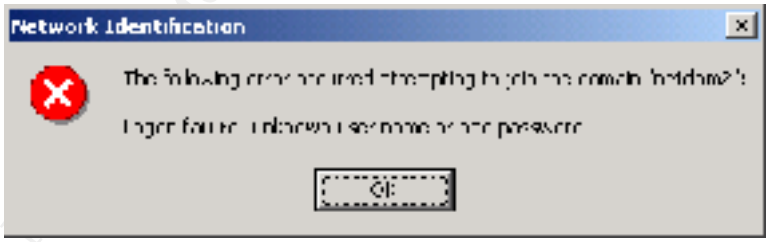

Figure 14 – Failure to Join the Domain

I was not able to make it work even by changing registry entries as suggested by some Microsoft Q articles. The problem goes away when you upgrade the Windows NT 4.0 primary domain controller to service pack 6a. If you have Windows NT 4.0 domain controllers running service pack 4 or earlier, consider upgrading them to service pack 6a. If this is not an option, you will need to configure the setting in the template to use NTLM authentication instead of NTLMv2. Double clicking the **LAN Manager Authentication Level** entry and making the change accordingly will allow you to make the change to NTLM.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

8. IMPLEMENTATION OF THE SECURITY POLICY TEMPLATE

Now we have a template ready to be used for system configuration. We will now configure the system we have been working on and then get ready to take the template to other systems.

Steps To Follow

1. To configure the current system, right click on **Security Configuration and Analysis** and click **Configure Computer Now…** You can change the location of the log location in the **Configure System** window to %windir%\security\logs if you like. This will make finding and reviewing them easier. It is also ok to accept the default in the **Configure System** window and click **OK**. It is up to you. When the **Configuring Computer Security** window comes up, wait till the configuration is complete.

2. To verify the configuration changes right click on **Security Configuration and Analysis** and click **Analyze Computer Now…** You can change the location of the log location in the **Perform Analysis** window to %windir%\security\logs if you like. This will make finding and reviewing them easier. It is also ok to accept the default in the **Perform Analysis** window and click **OK**. It is up to you. When the **Analyzing System Security** window comes up, wait till the analysis is complete. Expand the **Account Policies | Password Policy** section and the **Local Policies | Security Options** section to see the changed entries.

The system has now been configured using the security template that we created in earlier steps. Verify that the changes have been successfully set. In the graphics on the next two pages notice the differences between the before and after configurations. Notice the red X's versus the green check marks. Notice the Database Setting column versus the Computer Setting column.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

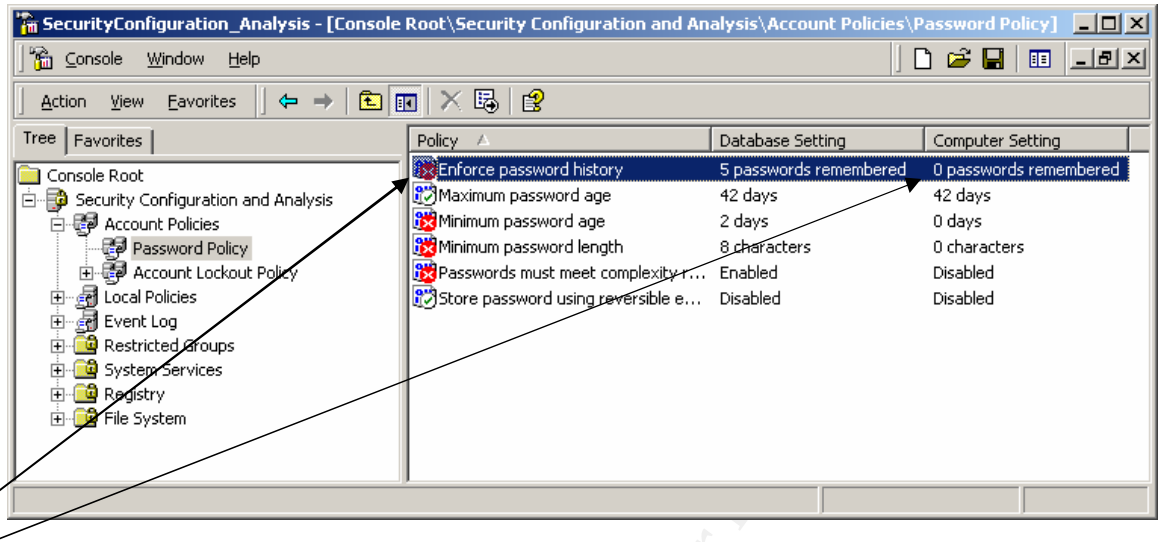

Figure 15 – Password Policy <u>Before</u> Configuration

Compare entries to note changes.

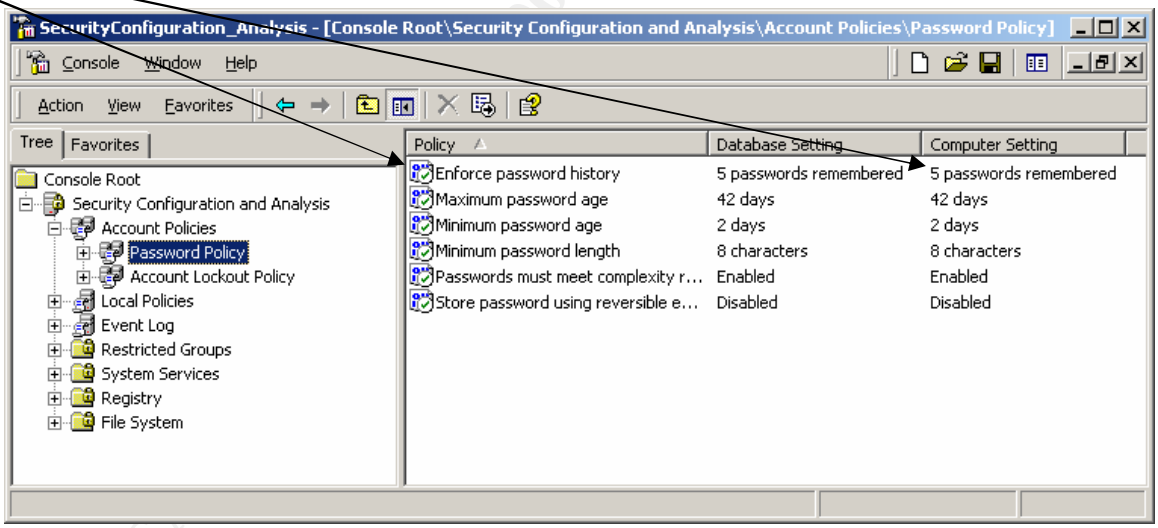

Figure 16 – Password Policy <u>After</u> Configuration

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

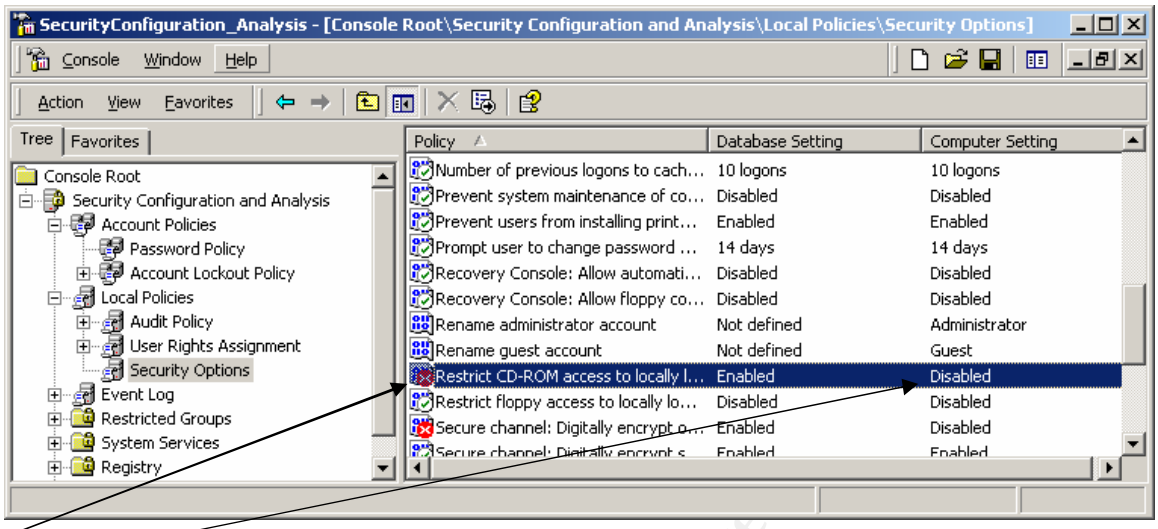

Figure 17 – Restrict CD-ROM Setting <u>Before</u> Configuration

Compare entries to note changes.

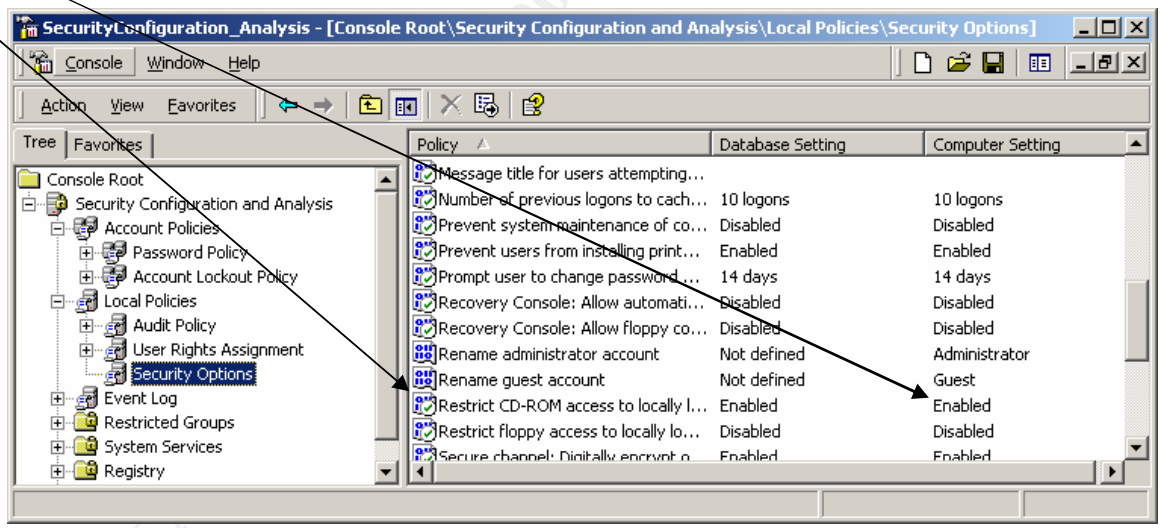

Figure 18 – Restrict CD-ROM Setting <u>After</u> Configuration

<u>You have now configured your first system.</u>

Once you are satisfied that the template successfully implemented the changes to this system, we can prepare to take the template to other systems. One nice way to accomplish this would be to create a simple script file. Let's look at doing that. Refer to the following graphic for the syntax.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

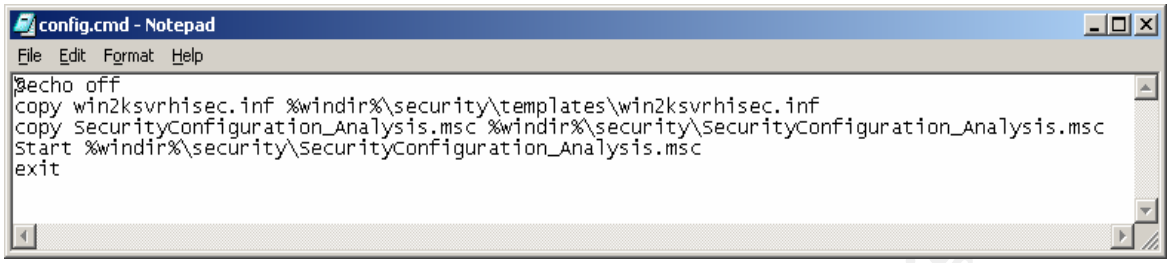

Figure 19 – Syntax of Script File

3. Locate the custom console (SecurityConfiguration_Analysis.msc) created in Section 6, Step 4., and the custom template (win2ksvrhisec.inf) that was created in Section 6, Step 9., and put them on a floppy or cdrom along with the above script file.

4. Take this floppy or cdrom to any **additional** systems that you would like to configure. Launch the script file (i.e. config.cmd) by double clicking it. This will copy the custom console and the custom template to the correct location on the system and launch the custom console. See graphic below for example.

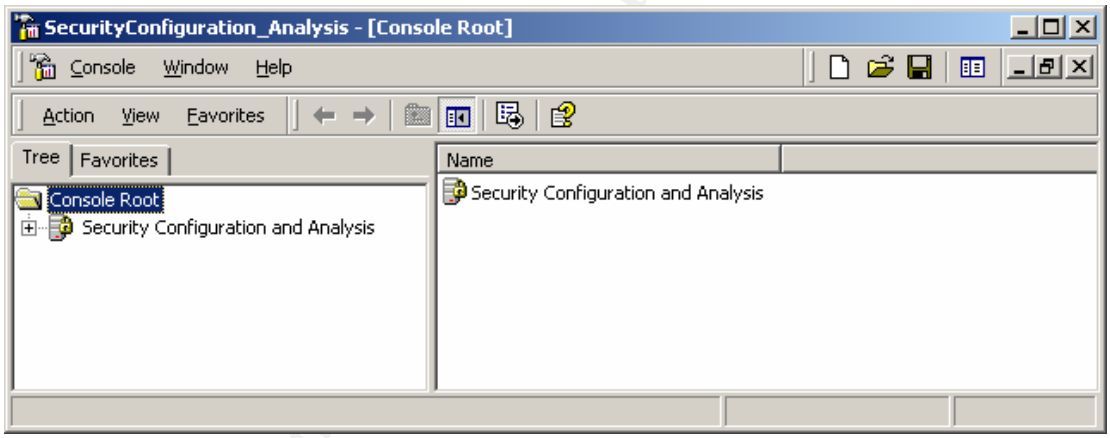

Figure 20 – Custom Console Launched From Script

From here the steps are similar to the ones we followed above but much more abbreviated because we don't need to set up the custom console or create and save the template. All that is necessary at this time is to configure the system based upon the parameters set in the template.

5. Right click on **Security Configuration and Analysis** and click **Open database…** In the **Open database** window in the **File name:** section type in an appropriate name (i.e. security.sdb) and then click **Open**. The custom template (i.e. win2ksvrhisec.inf) should appear in the **Import Template** window as one of the files. Click it and then click **Open**.

6. Right click on **Security Configuration and Analysis** and click **Configure Computer Now…** You can change the location of the log location in the

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Configure System window to %windir%\security\logs if you like. This will make finding and reviewing them easier. It is also ok to accept the default in the **Configure System** window and click **OK**. It is up to you. Wait while the **Configuring Computer Security** window completes.

7. The system can now be analyzed as was demonstrated above in Section 8. Step 2 to verify the correct application of the security template.

You can now configure as many systems as you need to using these few procedures.

9. SECEDIT COMMAND LINE TOOL

Windows 2000 has greater command line capabilities than all previous versions of Windows. The things that can be done from the Security Configuration and Analysis tool can also be done via the command line with a tool called SECEDIT.EXE. You can also use the Task Scheduler with it as well. There are 5 major operations that can be performed with this tool.

- Analyze
- Configure
- Export
- Refresh Policy
- Validate

We will list here the syntax for the Analyze, Configure, and Validate options.

The Analyze and Configure options in the command line tool are essentially the same as the Analyze and Configure Computer Now options in the Security Configuration and Analysis tool. The Validate option will check the template file for errors.[5]

Analyze system security

secedit /analyze

This command analyzes system security.

Syntax

secedit /analyze [**/DB** *filename*] [**/CFG** *filename*] [**/log** *logpath*] [**/verbose**] [**/quiet**]

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Parameters

/DB *filename*

Provides the path to a database that contains the stored configuration against which the analysis will be performed. This is a required argument. If *filename* specifies a new database, the **CFG** *filename* argument must also be specified.

/CFG *filename*

This argument is only valid when used with the **/DB** parameter. It is the path to the security template that will be imported into the database for analysis. If this argument is not specified, the analysis is performed against any configuration already stored in the database.

/log *logpath*

The path to the log file for the process. If this is not provided, the default file is used.

/verbose

Requests more detailed progress information during the analysis.

/quiet

Suppresses screen and log output. You will still be able to view analysis results using Security Configuration and Analysis.[6]

Configure system security

secedit /configure

This command configures system security by applying a stored template.

Syntax

secedit /configure [**/DB** *filename*] [**/CFG** *filename*] [**/overwrite**][**/areas** *area1 area2...*] [**/log** *logpath*] [**/verbose**] [**/quiet**]

Parameters

/DB *filename*

Provides the path to a database that contains the security template that should be applied. This is a required argument.

/CFG *filename*

This argument is only valid when used with the **/DB** parameter. It is the path to the security template that will be imported into the database and applied to the system. If this argument is not specified, the template already stored in the database will be applied.

/overwrite

This argument is only valid when the **/CFG** argument is also used. This specifies whether the security template in the **/CFG** argument should overwrite any template or composite template stored in the database instead of appending the results to the stored template. If this is not specified, the template in the **/CFG** argument will be appended to the stored template.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

/areas *area1 area2...*

Specifies the security areas to be applied to the system. The default is "all areas." Each area should be separated by a space.

Area Name	Description
SECURITYPOLICY	Local policy and domain policy for the system, including account policies, audit policies, and so on.
GROUP_MGMT	Restricted group settings for any groups specified in the security template
USER_RIGHTS	User logon rights and granting of privileges
REGKEYS	Security on local registry keys
FILESTORE	Security on local file storage
SERVICES	Security for all defined services

/log *logpath*

Path to the log file for the process. If not specified, the default is used.

/verbose

Specifies more detailed progress information.

/quiet

Suppresses screen and log output.[7]

Validate a security configuration file

secedit /validate

This command validates the syntax of a security template you want to import into a database for analysis or application to a system.

Syntax

secedit /validate *filename*

Parameters

filename

The file name of the security template you have created with Security Templates.[8]

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

10. ADDITIONAL READING

1. Microsoft Security Configuration Tool Set, White Paper, February Technet

2. Windows NT Security: Step-by-Step, SANS Institute

3. TSS/NSA Windows NT Security Guidelines, Steve Sutton, Trusted Systems Services, Inc.

4. Microsoft Knowledge Base Article ID: Q147706, How to Disable LM Authentication on Windows NT

11. CREDITS AND REFERENCES

[1] Microsoft White Paper, Default Access Control Settings in Windows 2000

[2] Microsoft Knowledge Base Article ID: Q238965, Removing Additional Permissions for Terminal Services Users

[3] Microsoft Windows 2000 Server Manual, Security

[4] Microsoft Knowledge Base Article ID: Q239869, How to Enable NTLM2 Authentication for Windows 95/98/200/NT

[5] Microsoft Step-by-Step Guide to Using the Security Configuration Tool Set, Technet, February 2001

[6] Windows 2000 Server, Automating Security Configuration Management Help utility, Analyze system security section under How To…

[7] Windows 2000 Server, Automating Security Configuration Management Help utility, Configure system security under How To…

[8] Windows 2000 Server, Automating Security Configuration Management Help utility, Validate a security configuration file under How To…

© SANS Institute 2000 - 2002 Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.