The Security Configuration Tool Set:

The Best Defense for Windows 2000

Martin Hardy
Version 2.1b

Table Of Contents

Introduction

This document provides a comparison of the tools used to secure both Windows NT 4.0 and Windows 2000 at the same time as detailing the usage of the Security Configuration Tool Set. Due to the number of security configuration options included in the Window 2000 tool set and the limited scope of this paper, the author has mentioned various configuration options, but not all. Many more options are available. Users are encouraged not only to use the templates provided by Microsoft and other agencies, but also to develop their own custom templates to configure systems with.

Although the author encountered few problems when configuring systems, it is stressed that thorough testing should be carried out before attempting to configure a production system.

The Problem

The integrity of a system is dependent upon the security of that system as a whole. A hacker may only needs to find the weak link in a one component to be able to exploit the whole system. Even after every effort has been taken to plug all holes and gaps within a system, some can still be overlooked and these can remain for the life of the machine.

Hacking tools specifically designed to search out multiple vulnerabilities in a systems are becoming user-friendlier. Tools such as L0phtcrack Version 3, Legion and SubSeven are being produced to look more like third party, professionally produced, weapons for hackers.

In order for a Windows NT server to be secured and still remain usable for its clients, Registry values have to be changed, modifications to the User Manager are required, and Windows Explorer is needed to properly configure permissions on sensitive files. The absence of a unified security program has caused most systems to remain vulnerable because most NT administrators don't take the proper steps in securing their systems. And even if they do, it's very easy to miss a crucial item or two.[1]

This can apply to even the most conscientious of administrators, especially when dealing with thousands of machines with differing images and applications installed.

[1] Harry Brelsford, "Service Pack 4 Additions and Miscellaneous". Windows IT Library. April 1999. http://www.windowsitlibrary.com/content/329/16/1.html

How to Defend the System

So, aside from employing third party tools to scan for vulnerabilities within the system what tools can an administrator use to defend his system?
The security of a properly locked down NT system is unquestionably high.
With Windows NT 4.0, Microsoft provided numerous tools such as User Manager, Server Manager, ACL Editor and Registry Editors to address different aspects of system security. Each tool provided an administrator with a graphical way of configuring various aspects of system security.

However these tools were not centralized. An administrator would have to open three or four applications to configure security for one computer. Many security conscious administrators therefore consider using these applications costly and cumbersome, in addition, security configurations can be complex.

The Beginnings of an Answer

The beginnings of an answer was introduced in 1998 as an additional component included in the Windows NT 4.0 Service Pack 4 CD-ROM. Microsoft had planned to stop including new features in the service packs, but NT 4.0 customers asked specifically for the Security Configuration Editor.

"One of the complaints about NT 4.0 was that it was not "locked down" out of the box," said NT product manager Karen Khanna, "This (Security Configuration Editor) will fix that". [2]

Security Configuration Editor (SCE) provided a centralized tool for an administrator to define and apply security configurations for Windows NT 4.0 workstations and Windows NT 4.0 server installations. SCE also gave the ability to inspect installed systems in order to locate any degradation in system security. Microsoft had provided a tool that did not feature any new security features or capabilities to Windows NT; it simply consolidated the many configuration settings available for NT. Included in this consolidation were most of the security parameters introduced through service packs and Hotfixes.

The concept of the Security Configuration Editor was simple. SCE was a template-based security editor capable of three basic functions: configuring security templates, applying a security template's setting to an NT system, and inspecting the security settings of an NT system by comparing those settings to the contents of a security template.

This was the fist step at change management for NT.

[2] Trot, Bob. "NT 4.0 Service Pack coming with NT 5.0 security Feature". InfoWorld Electric. February 27 1998.
http://archive.infoworld.com/cgi-bin/displayStory.pl?980227.whntpack.htm

The Drawbacks

The biggest drawback with the Security Configuration Editor for Windows NT 4.0 was that, when using the graphical interface, an administrator could only apply security configuration to one machine at a time.
This was of great use when configuring primary domain controllers or individual workstations but when it came to applying the same image to 10,000 clients on the network it was not very practical. Multiple hosts on Windows NT 4.0 could be evaluated and configured using a command line tool but this method would require more training and negates the simplistic nature of the Microsoft Management Console and Security Configuration Editor.

Requirements for the Installation of SCE on Windows NT 4.0

As the SCE was not initially intended for NT 4.0 additional software was needed to enable it to function. SCE is a snap-in for the Microsoft Management Console (MMC) so an administrator of an NT 4.0 system first needed to download MMC.
Upon attempting to run MMC the administrator received the prompt telling him that Internet Explorer was a prerequisite for running MMC. This could be enough reason to change the mind of the administrator who was not already running I.E. which has it's own security issues.
Many companies run Netscape and avoid running I.E. and Outlook because of the various vulnerabilities each has, and many administrators show understandable reluctance to install any applications that require them. However, as more and more vendors include I.E. as part of the installation requirements there seems to be a slow realization that I.E. is not optional, but a necessity.

Once installed the administrator would have a steep learning curve with both the Microsoft Management Console and the Security Configuration Editor snap-in. Combined with the fact that the administrator was used to using Explorer, Registry Editor and User Manager, the reasons for not attempting to centralize administration to one tool started to grow. Why should an administrator of an NT 4.0 system that seems to be secure, change his methods of managing users and securing the network?

For those administrators who think ahead it may seem more obvious. Windows NT 4.0 will not always be the operating system of choice. With the release of Windows 2000, more services are reliant upon the Microsoft Management Console. Vendors such as Symantec have now designed the Symantec System Center as a snap-in for MMC. An administrator who is already using SCE for Windows 4.0 will be ahead of the game with regard to both Windows 2X operating systems and with future applications from third parties.

Security Configuration Manager – Windows 2000

Windows 2000 includes the full tool kit named the Security Configuration Tool Set which is already becoming an invaluable tool for any administrator. Again Microsoft stress that the tool set is not intended to replace the User Manager, Server Manager and Access Control List Editor, rather, its goal is to complement them by defining an engine that can interpret a standard configuration file and perform the required operations automatically in the background. Administrators can continue to use existing tools to change individual security settings whenever necessary.

The SCM shipped with Windows 2000 is not the same as the SCM shipped on the CD-ROM Service Pack 4 for Windows NT 4.0.
There is no need for the installation of further applications such as Internet Explorer and the Microsoft Management Console as they are already included in the basic setup of Windows 2000.
Windows 2000 version of SCM includes additional features such as the capability to assessing security descriptors that apply to the objects in the Windows 2000 Active Directory and the ability to remotely analyze systems and apply security settings through the graphical user interface.

The Security Template and the Security Configuration and Analysis snap-ins, provide a centralized easy to use method of administering Windows 2000 security. The tools let you analyze your security settings by comparing them with the defaults, and to export the security templates you create for use in other machines on a network. With the Windows 2000 version of SCM the tools enable you to configure security at local machine level, or to amend a machine-type specific template that can then be applied to every machine of that type (workstation, member server and so on) in your network.
The security configuration tools are designed to meet the need for central security configuration, and to provide enterprise-level security analysis.

The tools set allows system administrators to consolidate many security-related system settings into a single configuration file (commonly referred to as a template or inf file because of the file extension .inf).

Microsoft has design the system so that it is possible to layer security configuration files to adjust for different software applications and security settings. As the role of a machine changes or as new applications are installed, a new configuration file can be applied to the machine through the incremental use of security policy templates. These security settings can be applied to any number of Windows 2000 machines either as part of a Group Policy Object (GPO) or through local computer configuration.

So How Does it Work?

The tools are designed to enable you to perform configuration at a macro level. By designing a template for a machine that will carry out certain tasks, the same template can be applied to any number of machines in the network. With NT 4.0 this process is carried out using numerous tools to change registry entries, change user rights and lock down shares, with SCM it becomes a point and click operation through the use of the one tool. The tools also provide micro management of individuals and machines at a local policy level.

To provide comprehensive security administration and information, the security configuration tools enable you to configure and analyze all of the following:

- **Account policies**—Through the account policies an administrator can configure local accounts on the local computer or domain accounts at the domain. Using a Domain Account policy an administrator can define password settings such as the required complexity, maximum/minimum age etc. (these parameters were previously set in User Manager), account lockout settings and the Domain Kerberos policy:

The options for Domain Kerberos are:

Enforce user logon restrictions - If the user does not have the appropriate user right, a service ticket will not be issued.

Maximum lifetime for service ticket – this determines the number of minutes a Kerberos service ticket is valid. The value for the default domain Group Policy Object (GPO) is set to 60 minutes.

Maximum lifetime for user ticket – this determines the number of hours a Kerberos ticket-granting ticket (TGT) is valid. This value is set to 10 hours in the default domain GPO.

Maximum lifetime for user ticket removal – Sets the maximum number of days that a user's TGT can be renewed. This value is set to 7 days in the default domain GPO.

Maximum tolerance for computer clock synchronization – this sets the maximum time a Kerberos Domain Controller and a client machine's clock can differ. An important factor in preventing replay attacks. The default value is 5 minutes.

- **Local policies**—The defined local policy is local to the specific machine, whether it is a workstation or server. Controls can be set on auditing, User rights and privileges and other locally configured options. Through the use of the auditing policy an administrator can select what events should be recorded, (the administrator should always bear in mind that the more auditing done on a system, the more system resources are used.)
  User rights assignment on a local policy controls the rights and privileges only on that specific system.

- **Event Log** – The settings that were controlled through Event Viewer in Windows NT 4.0 can now be controlled though the Event log configuration tool. The maximum log size, guest access restriction and how the information is stored can all be set here.

- **Restricted Groups**—The predefined groups such as Administrators, Power Users, Server Operators etc. can be managed using this tool. The administrator can also add groups with special privileges in order to track them via system configuration rather than user manager.

- **System Services**— Through the use of this tool, general settings for a wide range of services can be set. Settings include the service startup mode and the security on the service.

- **File or folder sharing**— Simply by viewing the template in the Security and Analysis tool an administrator can see what security settings are applied to any file or folder. The administrator can then specify changes to these settings.

- **Registry**— Includes registry key Discretionary Access Control List (DACL) settings (i.e., set the security on system registry keys.)
  The Registry keys can be set, simply by applying the security configuration and overwriting them or they can be set to inherit their settings.
  Due to the complexity and the effect that registry key changes can have on a system, a great deal of thought should be given before carrying out any modifications to the registry settings on a production environment.

- **System store**—used to set the security for local system file volumes and directory trees

- **Directory Security** –use this tool set to manage the security on objects residing in Active Directory

- **Predefined configurations** – Use these configurations as shipped, or use them as a starting point for building you own customized configurations. The configuration editing tool or Security Template snap-in provides this capability.

How easy are the Tools to Use?

These tools are designed to reduce costs associated with administering security on a network, therefore the tools have to be easy to learn and use. Once an administrator has experienced the use of the Microsoft Management Console, the snap-in tools start to look familiar.
The Microsoft Management Console is basic and should be familiar in appearance and usage to anyone who has used Windows Explorer over the last few years, with tree structures appearing on the left, and data screens on the right. Right click menu options abound, as do context-sensitive operations and help. Although the MMC's integrated, customizable console represents a marked improvement over the various screens and menus presented by the array of administrative tools in Windows NT 4.0, there are still areas with room for improvement. For example, one complaint frequently raised by administrators is the MMC's lack of drag and drop functionality.
For administrators new to MMC, Microsoft has provided the "Step-by-Step Guide to Using the Microsoft Management Console". [3]

Whether they are the snap-in tools for monitoring Norton Antivirus or the Security Configuration Tool Set, no superfluous graphics or statistics are included. Only a simple tabular view of the information with flags to show potential security problems. Microsoft also include the command line option to apply a configuration and perform analyses, this allows administrators to fit the tool easily into an existing administration model.

Security Analysis and Configuration Via the Command Line

The security configuration command line tool (secedit.exe) is all that is needed to perform a security analysis and to apply a security configuration to a Windows 2000 system. System analysis and configurations can be executed via batch file or scheduled programs; also, analysis results can be redirected to a file for review at a later time.
The command line option allows for analysis of individual security areas versus the entire configuration file The command line tool is also useful for applying predefined configuration files to many systems using distributed systems management tools.
The syntax of the command line is:

```
secedit {/analyze | /configure} [/cfg filename] [/db filename]
[/log LogPath] [/verbose] [/quiet] [/overwrite] [/areas Areas]
```

Table 1 explains the different options available:

/analyze	Performs an analysis
/configure	Performs a configuration
/cfg filename	Path to a configuration file to append to the database before performing an analysis.

[3] "Step-by-Step Guide to Using the Microsoft Management Console". http://www.microsoft.com/technet/win2000/mmcsteps.asp

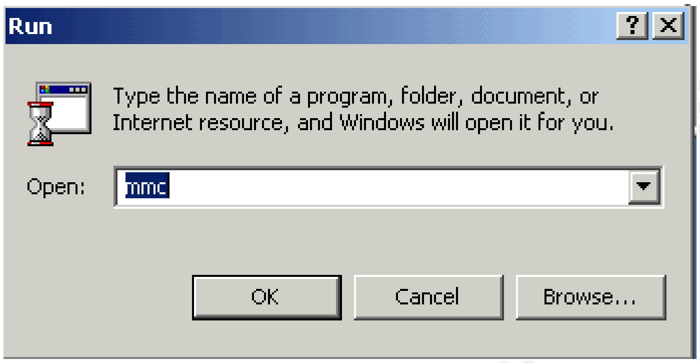
/db filename	The database that secedit will perform the analysis against.
/log LogPath	Path for the log fault – if this is not specified the log information will be output to the console.
/verbose	Provides detailed progress information
/quiet	Provides no log or screen output
/overwrite	Overwrites the database with the latest configuration information
/areas AREAS	This option is only relevant in conjunction with the /configure switch. The following areas are available: **SECURITYPOLICY** - Local policy and domain policy for the system. **GROUP_MGMT** - Restricted Group settings **USER_RIGHTS** - User rights assignments **DSOBJECTS** - Security on directory objects **REGKEYS** - Security permissions on local registry keys **FILESTORE** - Security permissions on local file system **SERVICES** - Security configuration for all defined services
/export	Exports a template from a security database to a security template file
/refreshpolicy	Reapplies a Group Policy Object to refresh security settings. The options available are: Machine_policy User_policy /enforce – This option reapplies settings whether they have been changed or not.
/validate	Validates the syntax of a template prior to importing into a database for analysis or configuration

Table 1 - Parameter syntax for secedit.exe options.

The main command line functions used to configure a system and to analyze a system are discussed in detail later in this document.

Using the Microsoft Management Console

MMC is loaded by default of Windows 2000 systems. To run the MMC, you can either create a shortcut somewhere, or simply use the "Start\Run" option, typing "MMC.exe" as shown in Figure 1.



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: mmc

Figure 1– MMC prompt

When you click "OK" you will be shown an empty console, into which you can add existing snap-ins as shown in Figure 2.

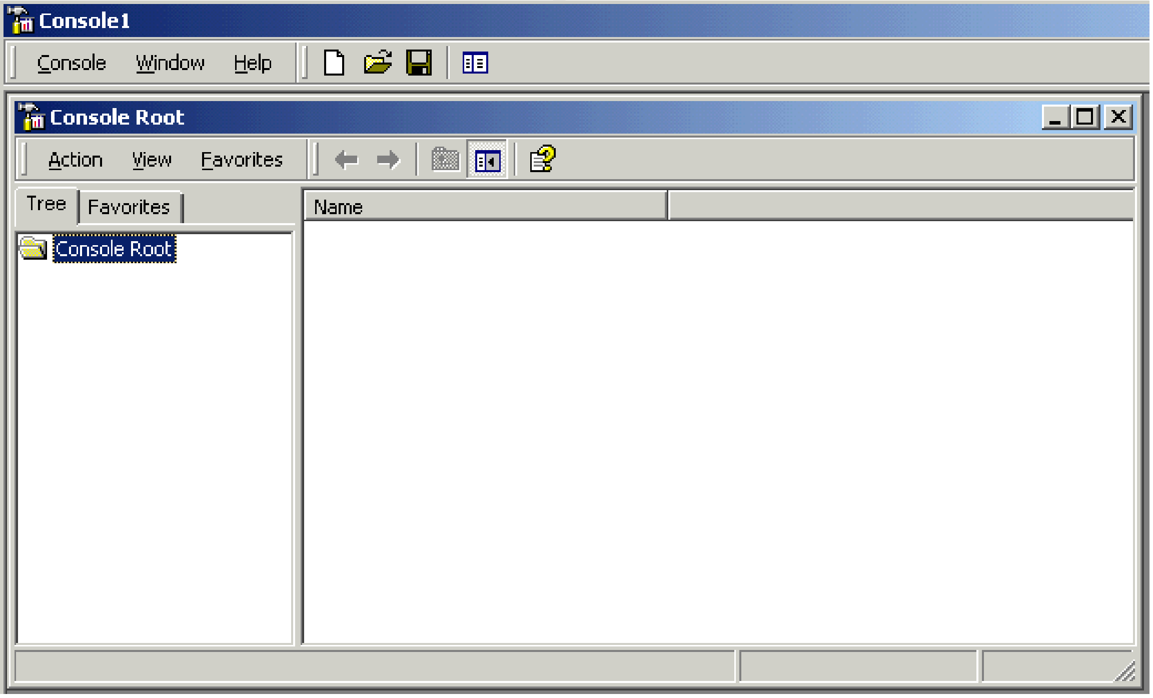
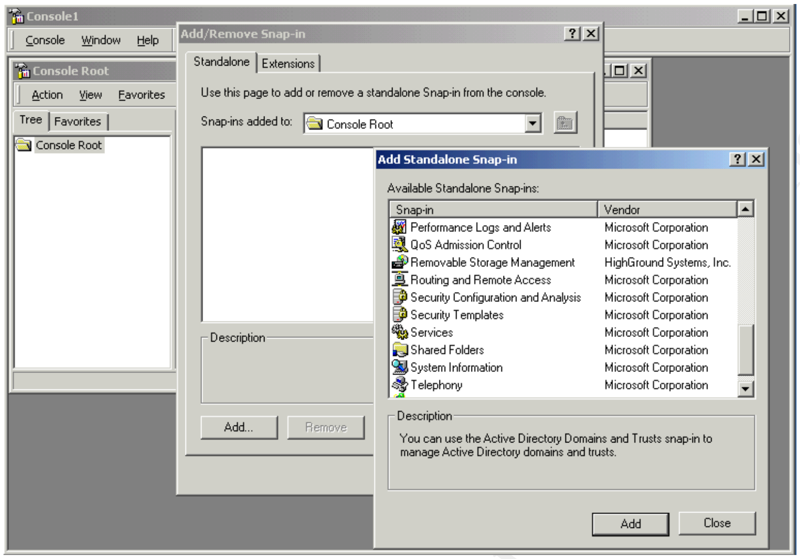


Figure 2 – Empty Microsoft Management Console.

To add snap-ins, select "Console\Add\Remove Snap-in," or press Ctrl-M within the

MMC. This takes you to the list of current snap-ins. If this is a new console, this list will be empty. Select "Add," and you are presented with the screen shown in Figure 3



Use this page to add or remove a standalone Snap-in from the console.

Snap-ins added to: Console Root

Description

Available Standalone Snap-ins:

Snap-in	Vendor
Performance Logs and Alerts	Microsoft Corporation
QoS Admission Control	Microsoft Corporation
Removable Storage Management	HighGround Systems, Inc.
Routing and Remote Access	Microsoft Corporation
Security Configuration and Analysis	Microsoft Corporation
Security Templates	Microsoft Corporation
Services	Microsoft Corporation
Shared Folders	Microsoft Corporation
System Information	Microsoft Corporation
Telephony	Microsoft Corporation

Description

You can use the Active Directory Domains and Trusts snap-in to manage Active Directory domains and trusts.

Figure 3 – MMC Snap-in Options

To load the Security Configuration and Analysis snap-in:
Select **Add**
Select **Security Configuration and Analysis**
Select **Add**
Select **Close**
Select **OK**

Figure 4 shows the MMC with the Security Configuration and Analysis snap-in loaded.

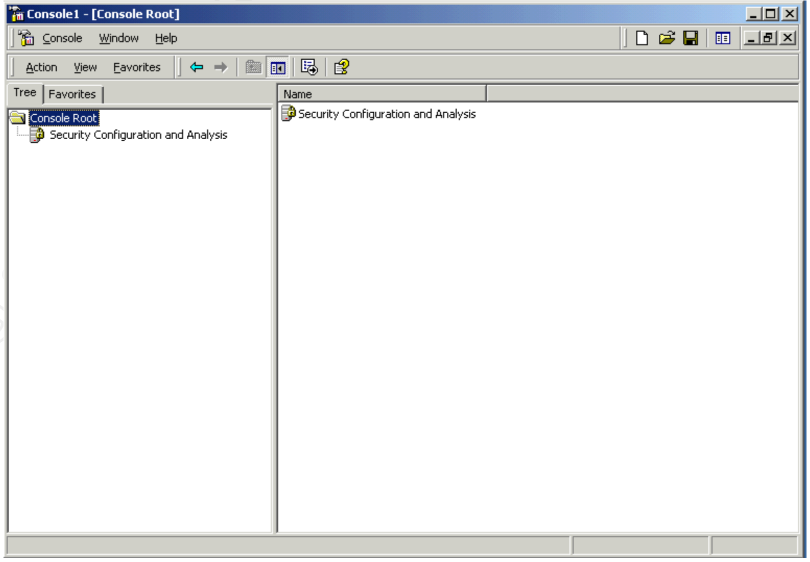

Console1 - [Console Root]
Console
Window
Help
Action
View
Favorites
Tree
Favorites
Console Root
Security Configuration and Analysis
Name
Security Configuration and Analysis

Figure 4 – MMC with Security Configuration and Analysis Tool snap-in

To configure a template to apply to a machine, the Template snap-in tool must be loaded into the MMC.

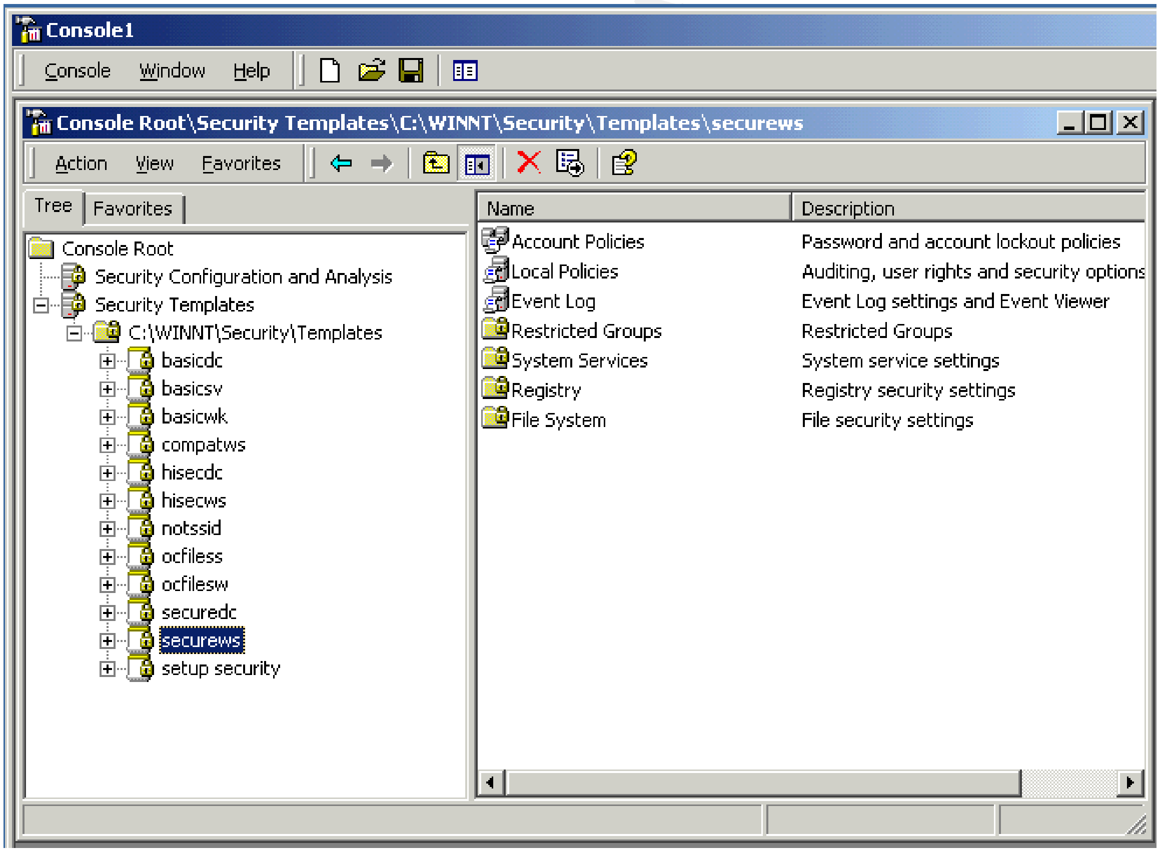
Security Templates

Security templates are files that contain a set of security configurations. The Security Templates snap-in must be loaded into the Microsoft Management Console (MMC) .the

To load the Security Templates snap-in:

Select **Console – Add/Remove Snap-in**
Select **Add**
Select **Security Templates**
Select **Add**
Select **Close**
Select **OK**

Figure 5 shows the MMC with the Security Configuration and Analysis and Security Templates snap-ins loaded.



Console Root\Security Templates\C:\WINNT\Security\Templates\securews

- Console Root
  - Security Configuration and Analysis
  - Security Templates
    - C:\WINNT\Security\Templates
      - basicdc
      - basicsv
      - basicwk
      - compatws
      - hisecdc
      - hisecws
      - notssid
      - ocfiless
      - ocfilesw
      - securedc
      - securews
      - setup security

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

Figure 5 - MMC with the Security Configuration and Analysis and Security Templates snap-ins loaded

In figure 5, one of the templates has been highlighted to show the options available to

configure.
The console settings can be saved by selecting **Save** in the **Console** menu, by default this is saved in the Administrative Tools menu of the currently logged in user. Enter the file name that you wish to save the console setting under and select **Save**. This avoids having to reload the snap-in every time MMC is closed and re-opened.

Security Templates in Windows 2000

Microsoft provides templates, which address various levels of security.
Table 2 shows a list of the templates included with the Windows 2000 Security Configuration Manager Tool Set.

File Name	Platform	Description
basicwk.inf	Windows 2000 Professional	Basic Workstation
basicdc.inf	Windows 2000 Server	Basic Domain controller
basicsv.inf	Windows 2000 Server	Basic Server
securedc.inf	Windows 2000	Secure Domain controller
securews.inf	Windows 2000 Professional	Secure Workstation
hissecdc.inf	Windows 2000 Server	Highly secure domain controller
hisecws.inf	Windows 2000 Professional	Highly Secure Workstation
notssid.inf		Specialized use. [4]
ocfiless.inf	Windows 2000 Server	Optional Component File Security. [5]
ocfilesw.inf	Windows 2000 Workstation	Optional Component File Security
setup security.inf	Windows 2000 Server	Default setup template

Table 2 – Microsoft Windows 2000 Templates

The Basic templates specify default security settings for all security areas, with the exception of user rights and group membership.

A Local Computer Policy database is initially created during setup on every computer with a clean installation of Windows 2000.[6] The template named Setup Security contains this initial database

The Secure templates provide increased security for areas of the operating system that are not covered by permissions, including increased security settings for the account policy,

[4] The notssid.inf template is specifically designed to remove Terminal Servers Users SID from the system
[5] The ocfiless and ocfilesw files add security settings for optional components. Options components are items like terminal services and certificate services that are not added to Windows 2000 systems when they are installed.
[6] Note: This is not the case when a Windows NT 4.0 or earlier-based machine is upgraded because a customer may have customized the security configuration, which must not be overwritten, In this case, the customer can use the Configure option of the tool set to apply a configuration.

increased settings for auditing, and increased security settings for some well-known security-relevant registry keys. This template does not modify access Control Lists (ACLs), because the assumption is that default Windows 2000 security settings are in effect.

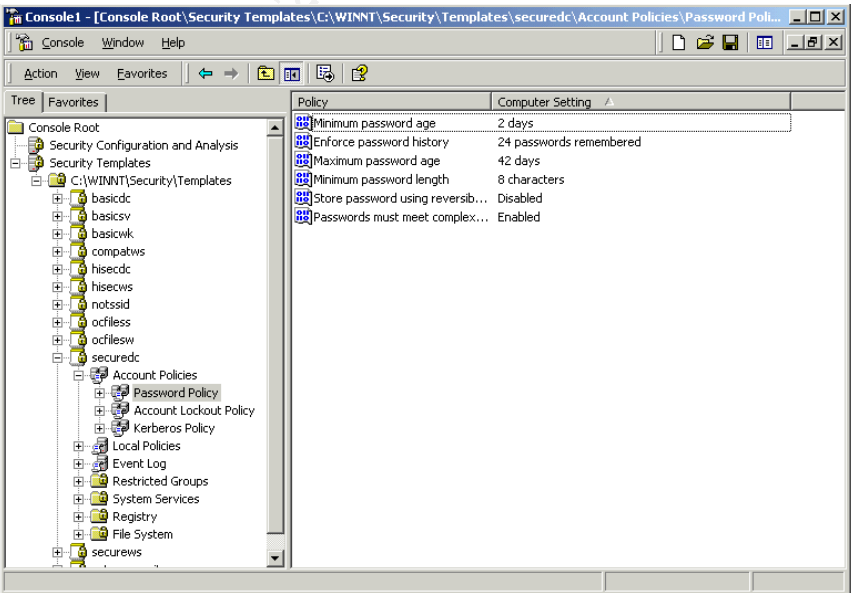
The Highly Secure templates are provided for Windows 2000-based computers that operate in native Windows 2000 environments. These templates require all network communications to be digitally signed and encrypted at a level that can only be provided by Windows 2000. Computers configured with this template cannot communicate with down-level Windows clients.

One other configuration provided by Microsoft but not considered suitable for a secure environment is Compatws.inf (Windows 2000 Professional). The Compatible template opens up the default permissions for the Local Users group so that legacy programs are more likely to run.

Steps to Applying a Template

Configuring a Template

By expanding the Security Templates menu in MMC select a template that suits the needs of the environment. By expanding the menu within the template an administrator can pick and choose which options he wishes to keep or change in the configuration. This is shown in figure 6, where the secure domain controller template (securedc.inf) has been selected and the Password Policy is configurable after expanding the Account Policies item.



Policy	Computer Setting
Minimum password age	2 days
Enforce password history	24 passwords remembered
Maximum password age	42 days
Minimum password length	8 characters
Store password using reversib...	Disabled
Passwords must meet complex...	Enabled

Figure 6 – Password Policy Options for Secure Domain Controller Template

After the changes have been applied the administrator should save the template using a different filename as the original; this will keep the templates in their original state in case they are needed at a later date. By default the templates are stored in the C:\WINNT\Security\Templates directory.

Applying the Template
In order to apply a template an administrator must first create a database to import the template to.

To Create a New Database

1. Right-click on the *Security Configuration and Analysis* scope item
2. Click **Open Database**
3. Type a new database name, and then click **Open**
4. A security template can then be selected, this will not configure the machine immediately, but will give the administrator the choice of either configuring the computer or analyzing the computer security settings.

To Configure the System via the GUI

1. Right-click the *Security Configuration and Analysis* scope item
2. Select **Configure Computer Now**
3. In the dialog, type the name of the log file you wish to view or leave the default value set, then click **OK**.

After configuration is complete, the administrator must perform an analysis to view the information in the database.

Configuring a System via the Command Line

To configure all of the available security options at one time via the command line:

```
secedit /configure [/cfg filename] [/db filename] [/log
LogPath] [/verbose] [/quiet] [/overwrite] [/areas Areas]
```

Following is an example of using the command line tool to configure only specific security areas:

```
secedit /configure /cfg “W2K workstation.inf” /db newdb.sdb /log logfile.txt /overwrite
/areas REGKEYS FILESTORE
```

This example will import the “W2K workstation.inf” file system and registry permission security settings and configure the local system.

Creating Additional Templates

In addition to the templates Microsoft supply with Windows 2000, other security configuration files can be customized for a particular environment. With the Security

Configuration Editor an administrator can define configuration files with prescribed security settings for each area of security. Through a graphical user interface the administrator can even cut and paste parts of configurations from different files to create a new customized configuration.

National Security Agency Templates

The National Security Agency has also made available security configuration files that comply with the Agency's recommended security settings for Windows 2000. [7]
They can be found through the following URL:
http://nsa1.www.conxion.com/win2k/index.html

Table 3 describes the templates provided by the National Security Agency

File Name	Platform	Description
W2K DC.inf	Windows 2000 Server/Advanced Server Domain Controller	Enhanced security settings for Windows 2000 domain controllers
W2K Workstation.inf	Windows 2000 Professional	Enhanced security settings for Windows 2000 workstations
W2K Server.inf	Windows 2000 Server/Advanced Server	Enhanced security settings for Windows 2000 member or standalone servers
W2K Domain Policy	Windows 2000 domain	Enhanced account policy settings to be applied in a domain-level Group Policy Object

Table 3 Enhanced Security Configuration Files

Security Analysis

The state of the operating system and applications on a computer is dynamic. For example, security levels may be required to change temporarily to enable immediate resolution of an administration or network issue: this change can often go unreversed, this means that a computer may no longer meet the requirements for enterprise security. Regular analysis enables an administrator to track and ensure an adequate level of security on each computer as part of an enterprise risk management program. Analysis is highly specified: information about all system aspects related to security is provided in the results. This enables and administrator to tune the security level and, most importantly, detect any security flaws that may occur in the system over time.

Security Configuration and Analysis Database

[7] National Security Agency "Windows 2000 Security Recommendation Guides"
http://nsa1.www.conxion.com/win2k/index.html

The security configuration and analysis database is a computer specific data store that is generated when one or more configurations are imported to a particular computer. There is an initial database created from a clean installation of Windows 2000. Initially this database will contain the default security configuration of the system. There are several security template files that contain the default security settings applied to a clean-install (non-upgraded) Windows 2000 machine. These files are hidden by default and reside in the %SystemRoot%\inf folder. Table 4 shows a list of the default security templates.

File Name	Platform
Defltdc.inf	Windows 2000 Server/Advanced Server Domain Controller
Defltsv.inf	Windows 2000 Server/Advanced Server
Defltwk.inf	Windows 2000 Professional

Table 4 Default Security Configuration Files

An administrator should export this configuration to a security configuration file, and save it. This file can later be used to restore initial security configuration at any later point. A security configuration and analysis database is the starting point for all configurations and analysis done on a system

The default security templates are especially useful when converting from a FAT or FAT32 file system to NTFS. When a conversion is made the default settings on the file system default to the "Everyone" group having full control over all files and folders. To obtain the file system security settings that would have been present if NTFS had been the original file system, an administrator can apply the File System portion of the appropriate default security template.

The local computer policy database defines the security policy in force for that system. Policy may not define the entire configuration; various configuration attributes can be ignored. Attributes that are not enforced by policy may also be configured manually using personal databases. However any custom configurations that conflict with the policy are overridden by the definitions in the policy.

To Analyze the Computer Security Settings

1. Right-click the *Security Configuration and Analysis* scope item
2. Select **Analyze Computer Now**
3. In the dialog, type the log file path, and then click **OK**

Note: To view the log file created during a configuration or analysis, select **View Log File** on the *Security Configuration and Analysis* context menu.

Performing a Security Analysis via the Command Line
To perform a security analysis via the command line, execute the following in a CMD

prompt window:

```
secedit /analyze [/cfg filename] [/db filename] [/logLogPath] [/verbose] [/quiet]
[/overwrite] [>> Analysis.file]
```

Analysis_file is the name of a file to contain the analysis results. This is useful for reviewing the results at a later time. If the >> *Analysis_file* is omitted, output will be written to the screen.

To Compare the Computer Security Settings against Another Security Template

1. Right-click the *Security Configuration and Analysis* scope item
2. Select Import Template, and choose template you wish to compare the computer settings to
3. Right-click the Security Configuration and Analysis scope item
4. Select Analyze Computer Now
5. In the dialog, type the log file path, and then click OK

The system will be analyzed against the template. The results of which are useful for:

a) Assessing the different security policies that would be applied if you choose to configure the system using another template.

b) Comparing the current configuration of a machine to the original configuration of that machine. This is useful in both troubleshooting and when trying to detect if changes have been made to a machine.

Figure 7 shows the type of results obtained from an analysis of the current system compared with a highly secure domain controller template.

Figure 7 – Example of Security Configuration Analysis

Again to ease the administration effort the display is kept simple. Any anomalies are shown by a red circle with a white cross, all other settings that meet the template criteria are displayed as a white circle with a green check mark.

Applying a configuration to more than one System

Through the integration of the Security Configuration Tool Set with the Group Policy infrastructure is possible to employ the same technology used to configure local security policies on individual computers to define security policies for domains and organizational units in the Active Directory service.

This document does not cover the full procedures for applying a Security Configuration to a domains and Organizational Units. However the detailed process is included Microsoft TechNet Article, "Step-by-Step Guide to Configuring Enterprise Security Policies". [8]

The Group policy infrastructure allows you to set security policies within Group Policy Objects (GPOs). These GPO's are assigned to a domain or organizational unit within the Active Directory and can then be applied to all computers associated with the relevant GPO.

[8] Microsoft TechNet Article, "Step-by-Step Guide to Configuring Enterprise Security Policies". http://www.microsoft.com/TechNet/win2000/entsec.asp

A marked difference to note with Windows 2000 is the order of precedence for security policies. The order of precedence is as follows: Local Policy has the least precedence, Domain Policy and then the Organizational Unit containing the computer has the highest precedence. Therefore, domain policies take precedence over locally defined policies. This means that when policies are set for a domain, they affect every computer in that domain.

Conclusion

When you manage an operating system's security, you face two basic tasks: securing the system and making sure the system remains secure.
A well-defined security policy for a computer network is a sound basis on which to build. With the tool set Microsoft has provided with Windows 2000, an administrator can take that security policy and develop custom templates for the enterprise to enforce it. Subsequent analysis of the system, using the tool set will provide an administrator with a graphic presentation of new areas of weakness in the system or unauthorized changes. The Security Configuration Tool set provides the centralized and easily security management that was lacking in Windows 4.0.

Only some tools included in the tool set have been discussed in this paper, in addition Microsoft has designed both Microsoft Management Console and the Security Configuration Manager so that new tools can be added to the tool set in the future.

References:

Brelsford, Harry. "Service Pack 4 Additions and Miscellaneous." IDG Books. April 1999. URL:
http://www.windowsitlibrary.com/content/329/16/1.html

Microsoft Corporation. "Microsoft Security Configuration Manager for Windows NT 4 White Paper." November 13 1998. URL:
http://www.microsoft.com/ntserver/security/techdetails/prodarch/securconfig.asp

Trot, Bob. "NT 4.0 Service Pack coming with NT 5.0 security Feature". InfoWorld Electric. February 27 1998. URL:
http://archive.infoworld.com/cgi-bin/displayStory.pl?980227.whntpack.htm

Edwards, Mark. "Service Pack 4's New Security Configuration Editor", October 1998. URL: http://www.win2000mag.com/Articles/print.cfm?ArticleID=3842

Microsoft Corporation. "Microsoft Windows 2000 Server Security Configuration Tool Set White Paper." April 19 1999. URL:
http://www.microsoft.com/windows2000/techinfo/howitworks/security/sctoolset.asp

Microsoft Corporation. "Step-by-Step Guide to Using the Microsoft Management Console".
http://www.microsoft.com/technet/win2000/mmcsteps.asp

Schultz, E. Eugene. Windows NT/2000 Network Security. Indianapolis, Macmillan Technical Publishing, Aug. 2000.

Mclean, Ian. Windows 2000 Security, Little Black Book. Arizona, The Coriolis Group, 2000.

Haney, Julie M. "Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set." May 17 2000. URL:
http://nsa1.www.conxion.com/win2k/index.html

Microsoft Corporation. "Windows 2000 Security Templates Are Incremental" January 2 2001. URL:
http://support.microsoft.com/support/kb/articles/Q234/9/26.ASP

National Security Agency "Windows 2000 Security Recommendation Guides"
http://nsa1.www.conxion.com/win2k/index.html