



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 permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Securing Windows and PowerShell Automation (Security 505)"
at <http://www.giac.org/registration/gcwn>

**Configuring and Auditing Windows NT
With
Security Configuration Manager**

SANS GIAC Windows NT Security Practical Assignment
September 2000
Lisa Yeo

Table of Contents

Introduction	1
Define Configuration File	2
Account Policies	2
Local Policies	2
Event Log	3
Restricted groups	4
System Services	4
Registry	4
File System	4
Analyze Existing Configuration	6
Apply Configuration File	8
Ongoing Auditing Practices	8
Perform Regular Analysis	8
Perform Analysis after Major System Modifications	10
Considerations	10
References	11

Table of Figures

Figure 1: Sample configuration file before changes	2
Figure 2: Changing Audit logon events	3
Figure 3: Logon message text	3
Figure 4: Event log settings	4
Figure 5: Administrator restricted group dialogue box	4
Figure 6: Listing of restricted groups	4
Figure 7: Default settings on a new folder	5
Figure 8: Advanced access control settings	6
Figure 9: Database menu options	6
Figure 10: Security configuration analysis	7
Figure 11: Details of configuration file vs. actual settings mismatch	8

Introduction

This paper discusses the use of Microsoft's Security Configuration Manager (SCM) in configuring settings on an Internet Information Server 4.0 (IIS4) host. SCM can be used both to define the initial configuration and audit deviations from the original definition. Not all recommended settings for an IIS server are discussed here, nor can they be configured solely using the SCM. An initial guide to configuring IIS4 on Windows NT 4.0 can be found in [2].

Defining a security configuration file in SCM provides a centralized location for ensuring compliance with a corporate security policy. The security configuration file can be reviewed easily to ensure continued compliance as the security policy is altered to reflect changed business needs or best practices. Further, the configuration file becomes a baseline to measure the host's security settings against, allowing the system administrator to easily locate altered settings.

The steps discussed in the paper can easily be broken down into *** main categories.

- Define the configuration file that will be used on the host. This requires knowing the intended purpose of the host being secured, best practices for securing a host providing the specified services (in this case IIS4), and referring to any corporate security policy that may be in place. With this information, a sample security configuration file can be modified to meet the specific needs of the organisation.
- Analyze the existing configuration against the security configuration file that has just been defined. This will allow the system administrator to ensure that the settings in the security configuration file are indeed the correct settings for the system. It is possible when working from a template to miss, or misconfigure, an important setting. The security configuration file can be updated after the analysis to reflect an necessary, and allowable, changes.
- Apply the security configuration file. This sets the security configuration of the system to the defined baseline. This not only ensures that the host conforms to defined security requirements now, but allows for step four.
- Regularly audit the security configuration. Using the defined baseline the system administrator can run a regular analysis of the host to ensure on-going compliance. These audits can be automated through the use of a command line tool, but should also be run manually after major system configuration changes so that the system administrator is familiar with the effects of the changes.

Define Configuration File

Using corporate security policy and best practices documents available from several sources, evaluate the templates that come with SCM. Begin with the template most closely resembling your required configuration.

Create a copy of your chosen template by right-clicking and choosing Save As...
Changes will be made to this new template (seversecurity.inf)
Alter settings as necessary.

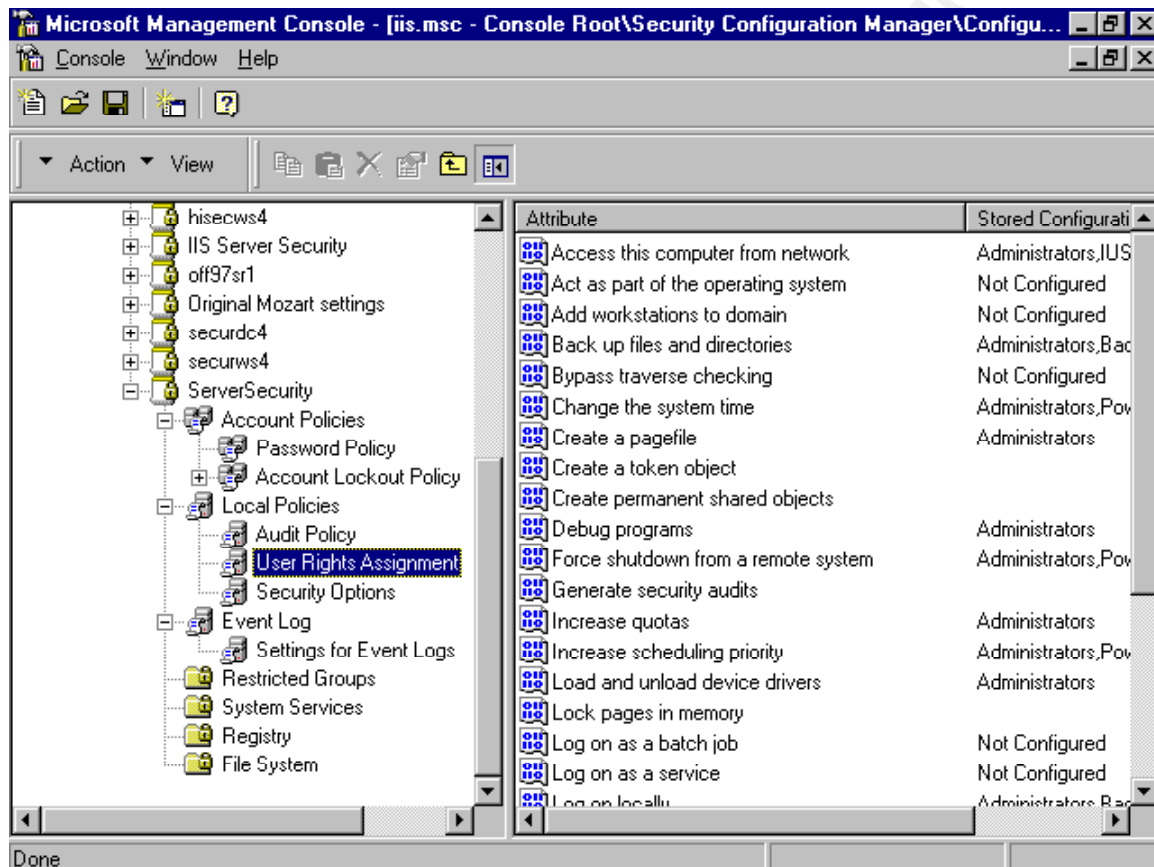


Figure 1: Sample configuration file before changes

Account Policies

Password policies

- Set password restrictions according to corporate security policy

Lockout policy-accept template defaults

- Set lockout parameters according to corporate security policy

Local Policies

Audit Policy

- Turn on auditing. Set according to corporate security policy or best practices as defined in [1], whichever is more comprehensive.

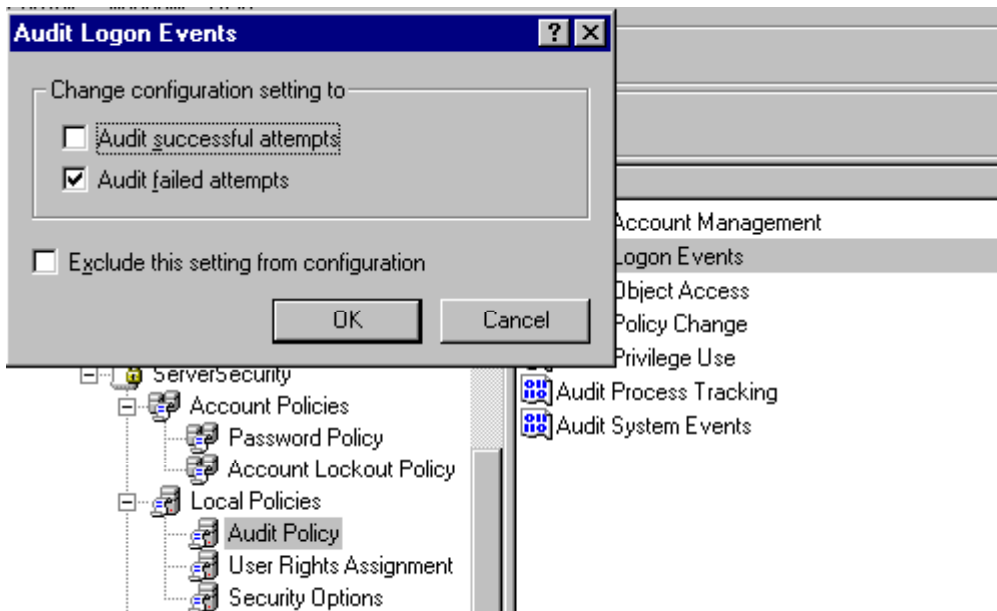


Figure 2: Changing Audit logon events

User Rights Assignments

- Restrict “Manage Auditing and Security log”
- Restrict logon over network right (remove IUSR_SERVERNAME if necessary)
-

Security Options

- Set logon information to not display last logon ID
- Set cached logons to zero
- Define logon message to warn users

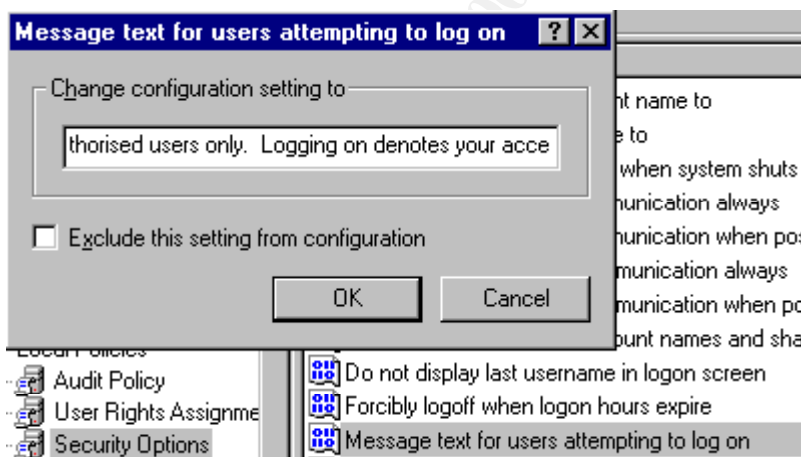


Figure 3: Logon message text

- Define logon title to warn users
- Enable “Do not display last username in logon screen”
- Enable auditing of backups and restores
- Define “Change Administrator account name to”

Event Log

This section configures the event log as you would manually do through User Manager

for Domains.

Configure event log settings according to corporate security policy.








Attribute	Stored Configuration
 Audit Account Management	Success,Failure
 Audit Logon Events	Success,Failure
 Audit Object Access	No Auditing
 Audit Policy Change	Success,Failure
 Audit Privilege Use	Failure
 Audit Process Tracking	No Auditing
 Audit System Events	Success,Failure

Figure 4: Event log settings

Restricted groups

Configure Administrator group to include only necessary users.



Figure 5: Administrator restricted group dialogue box

Configure other sensitive groups as necessary. Do not use SCM to define all group memberships.




Attribute	Membership	Member O
 Administrators	lvbeethoven,fchopin	
 FTP Users	wmozart,rwagner,ptc...	
 Webmasters	wmozart,cschumann	

Figure 6: Listing of restricted groups

System Services

It is possible to configure startup and security options for services. Configure according to corporate security policy.

Registry

The SCM contains pre-defined templates of registry access control lists (ACLs). These were reviewed when the starting template was chosen. Edit as required by corporate security policy.

File System

SCM contains pre-defined templates of NTFS settings. Modify as necessary to comply with corporate security policy.

- Configure ACL for ftp site

Right click File System and choose Add Folder...

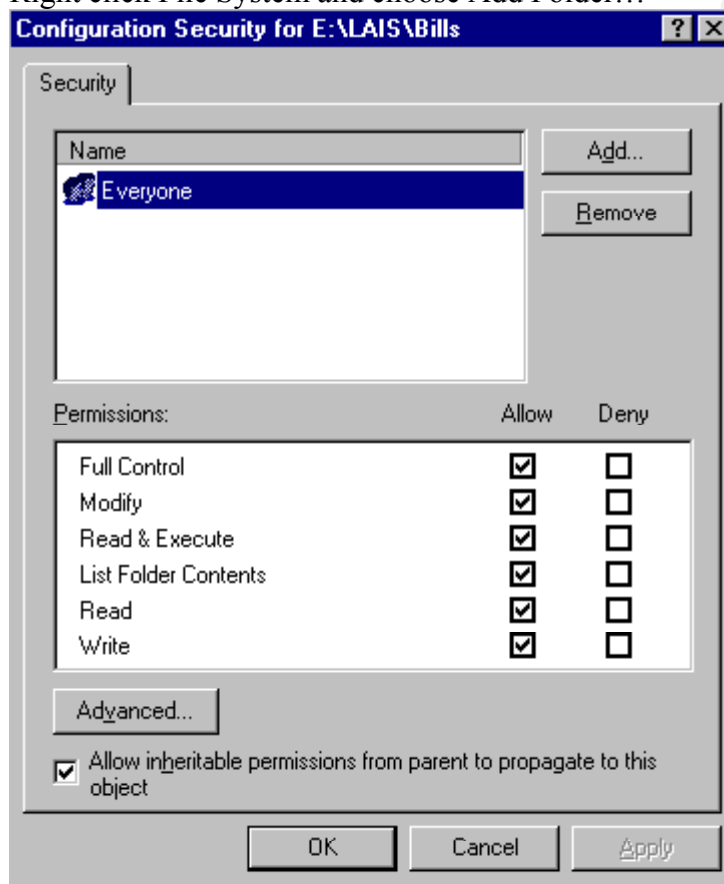


Figure 7: Default settings on a new folder

- Configure ACL for website

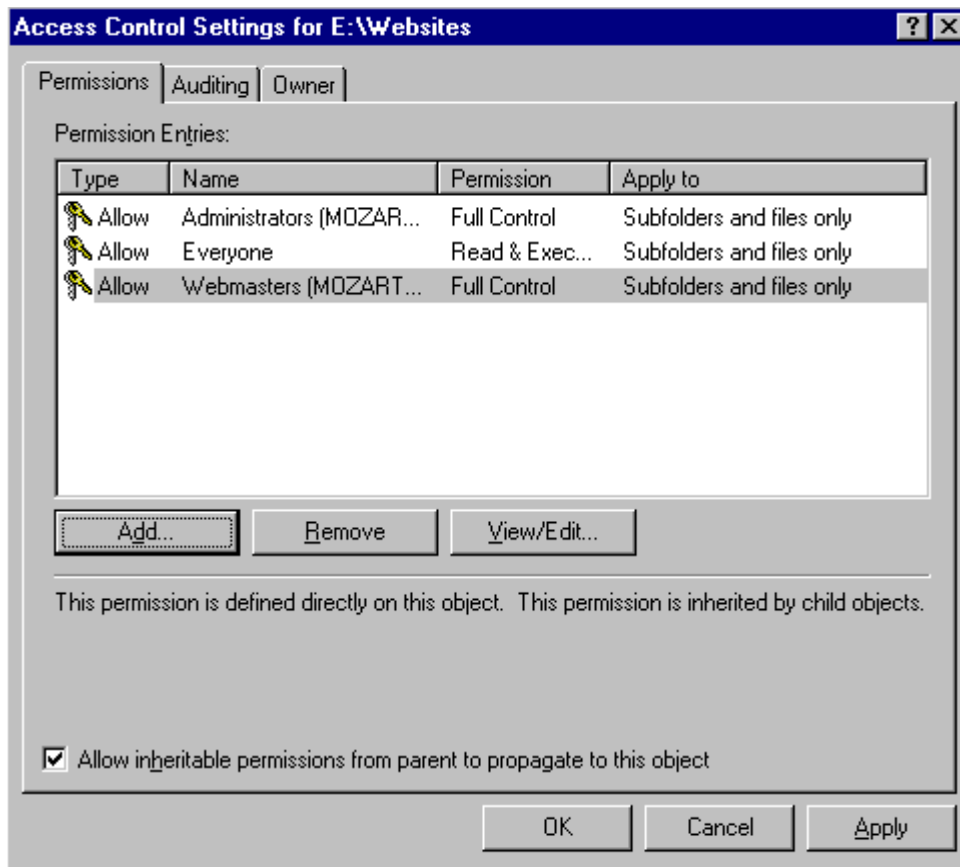


Figure 8: Advanced access control settings

- Check that event logs are secured and audited
(%systemroot%\system32\config*.evt)

Analyze Existing Configuration

Before applying the new configuration, use it to analyze the existing set up.

Right click Database and choose Import Configuration

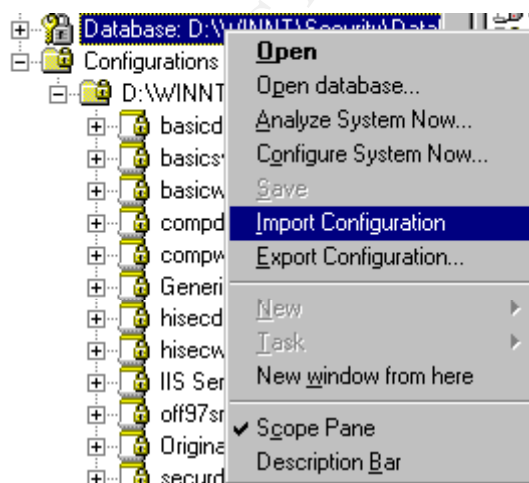


Figure 9: Database menu options

Choose the serversecurity.inf created above
 Right click Database and choose Analyze System Now

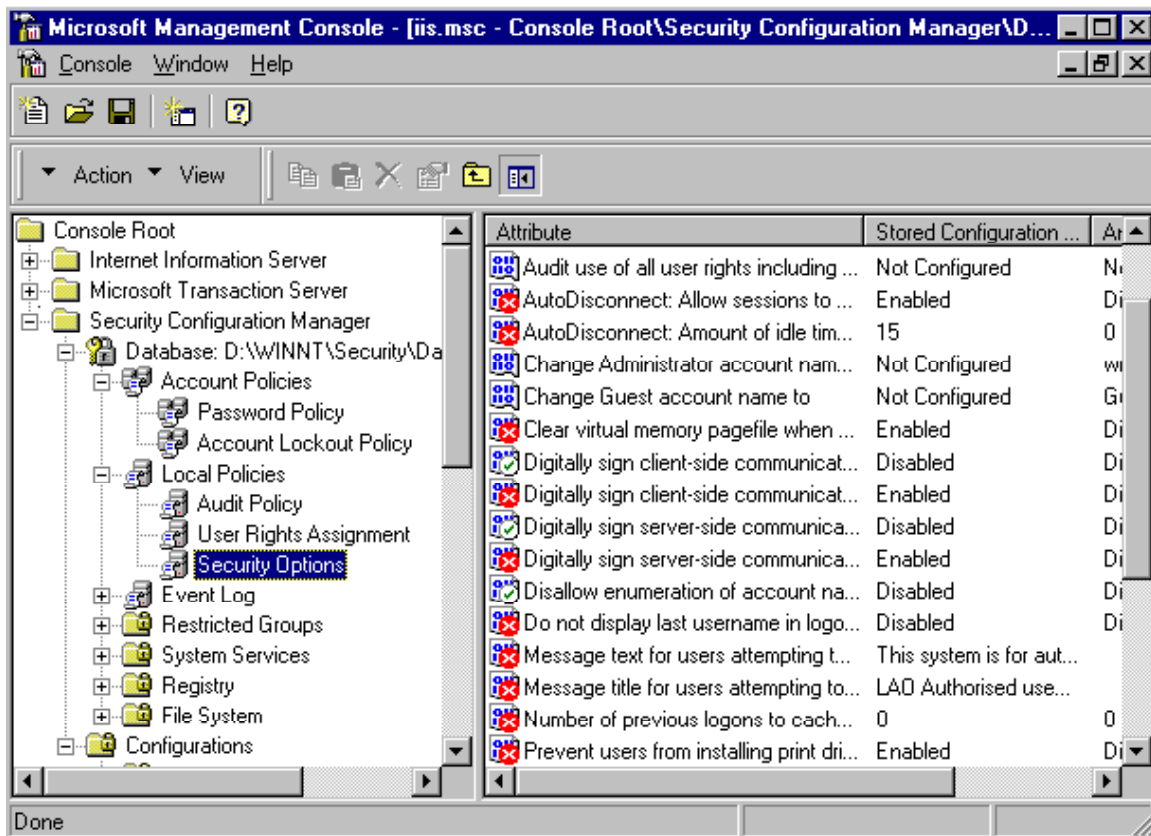


Figure 10: Security configuration analysis

Review all settings to determine if the configuration file is correct (vs. the analysis data).
 If appropriate, change the configuration setting to match the analyzed setting.

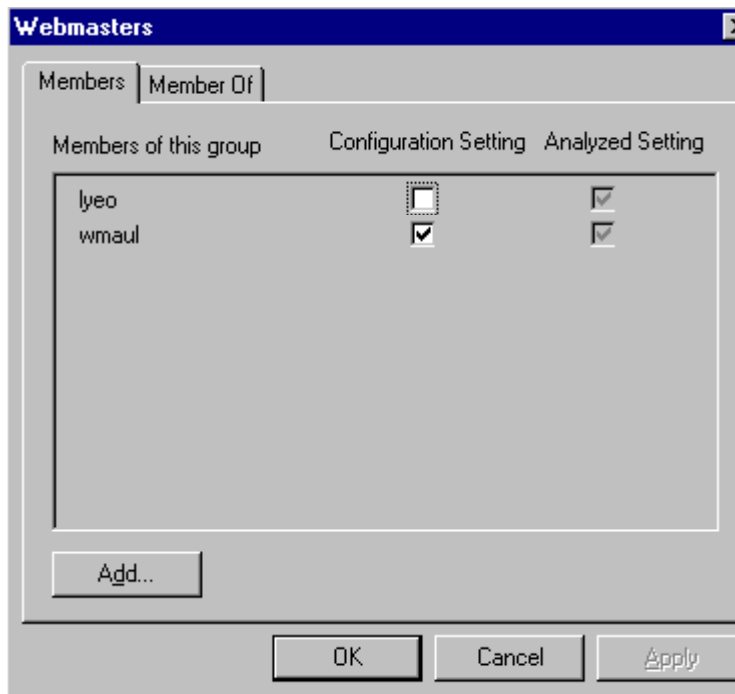


Figure 11: Details of configuration file vs. actual settings mismatch

When finished reviewing the analysis, export the configuration to ensure you have a copy of the correct configuration file.

Right click Database and choose Export Configuration

Apply Configuration File

To apply a configuration file, import it to the database using the instructions above. Right click Database and choose Configure System Now.

Ongoing Auditing Practices

The above steps ensure that the configuration of the system adheres to the defined security configuration at this time. However, it is possible for changes made by users/administrators to alter the security settings of a computer. To ensure continued adherence to the security objectives, regular analysis must be performed. There is a command line tool supplied with SCM that can aid in this task.

Perform Regular Analysis

Schedule the following command to run weekly (or as defined in Corporate Security Policy).

```
C:\> secedit /analyze /cfg
winnt\security\templates\serversecurity.inf /log e:\logs\analysis.log
/verbose
```

The analysis log must be reviewed for mismatched values.

Configuring and Auditing Windows NT with Security Configuration Manager Page 10

With this sample excerpt we can see that the members in the Administrator group do not match the define security configuration file. The GUI tool can show details of the mismatch as in Figure 10.

```
-----
Date: 09-14-2000   Time: 11:06:56
Initialize engine, please wait...
----Analysis engine is initialized successfully.----
    Event audit settings are turned off.
----Reading Configuration info...
----Analyze User Rights...
    Analyze SeNetworkLogonRight.
    Analyze SeTcbPrivilege.
Not Configured - SeTcbPrivilege.
    Analyze SeMachineAccountPrivilege.
Not Configured - SeMachineAccountPrivilege.
    Analyze SeBackupPrivilege.
    Analyze SeChangeNotifyPrivilege.
Not Configured - SeChangeNotifyPrivilege.
    Analyze SeSystemtimePrivilege.
    Analyze SeCreatePagefilePrivilege.
    Analyze SeCreateTokenPrivilege.
    Analyze SeCreatePermanentPrivilege.
    Analyze SeDebugPrivilege.
    Analyze SeRemoteShutdownPrivilege.
    Analyze SeAuditPrivilege.
    Analyze SeIncreaseQuotaPrivilege.
    Analyze SeIncreaseBasePriorityPrivilege.
    Analyze SeLoadDriverPrivilege.
    Analyze SeLockMemoryPrivilege.
    Analyze SeBatchLogonRight.
Not Configured - SeBatchLogonRight.
    Analyze SeServiceLogonRight.
Not Configured - SeServiceLogonRight.
    Analyze SeInteractiveLogonRight.
    Analyze SeSecurityPrivilege.
    Analyze SeSystemEnvironmentPrivilege.
    Analyze SeProfileSingleProcessPrivilege.
    Analyze SeSystemProfilePrivilege.
    Analyze SeAssignPrimaryTokenPrivilege.
    Analyze SeRestorePrivilege.
    Analyze SeShutdownPrivilege.
    Analyze SeTakeOwnershipPrivilege.

    User Rights analysis completed successfully.

----Reading Configuration info...
----Analyze Group Membership...
    Analyze Users.
Not Configured - Users__Members.
Not Configured - Users__Memberof.
    Analyze Webmasters.
    Analyze FTP Users.
    Analyze Administrators.
Mismatch      - Administrators__Members.

    Group Membership analysis completed successfully.

----Reading Configuration info...
```

Typing `secedit` with no options will provide the tool's syntax.

Perform Analysis after Major System Modifications

Use either the command line utility or the GUI interface. In this instance, the GUI tool may provide an advantage. The GUI interface allows for immediate comparison of non-complying values as well as updating of the configuration file where appropriate.

Considerations

- A script to search the weekly generated analysis log file for mismatch entries and then report any anomalies to the system administrator would be a valuable time saver.
- Cannot remotely configure hosts with the GUI utility, can only configure local machine.
- Can use the command line utility in scripts to configure remote hosts.

In summary, then, Microsoft's Security Configuration Manager is a useful tool in the system administrator's quest for maintaining a stable and secure environment. However, it cannot be the only tool used by an administrator. Tools such as Policy Editor provide better means of configuring client machines, Event viewer is still necessary, and while you can use SCM to set the requirement for strong passwords, you still need software to define the conditions of a strong password. The SCM is just one resource in a system administrator's toolkit.

References

- [1] SANS Institute. *Windows Security Step by Step v2.15*. The SANS Institute, 1999
- [2] Microsoft TechNet. "Microsoft Internet Information Server 4.0 Security Checklist." 15 March 2000. URL:<http://www.microsoft.com/technet/security/iischk.asp> (14 September 2000)
- [3] CERT Coordination Center. "Selecting Audit Events for Windows NT 4.0 registry keys". Improving Security. 17 March 1999. URL:<http://www.cert.org/securiyt-improvement/implementations/i028.04.html> (19 September 2000)
- [4] Microsoft TechNet. "Microsoft Security Configuration Manager for Windows NT 4 White Paper." 12 January 2000. URL:
<http://www.microsoft.com/technet/winnt/winntas/technote/scmnt4.asp> (21 September 2000)
- [5] Fossen, Jason, and Jennifer Kolde. *Securing Windows NT: Step-by-Step, Parts 1, 2 & 3*. The SANS Institute GIAC Training, 2000
- [6] Halprin, Geoff. *A System Administrator's Guide to Auditing*. The USENIX Association. 2000