Global Information Assurance Certification Paper

The Security Configuration Tool Set in Windows 2000 (Practical Exercise)

Submitted by:

Michelle Briggs

April 2, 2001

Table of Contents

1.0 Security Configuration Tool Set

Windows 2000 introduces a number of new security tools that make security configuration for administrators an easier and less time-consuming task. In Windows NT 4.0, many security configuration items have separate applications located throughout the operating system. Most of these items are in the User Manager for domains and require multiple graphical user interfaces (GUIs). The Windows 2000 Security Configuration Tool Set allows the administrator to easily configure and manage security policies for a single machine, an entire domain, or organizational unit within a single GUI. Security Configuration Tool Set answers the administrator's need for a central security configuration tool. Most importantly, it reduces security-related administration costs by defining a single point where the entire system's security can be viewed, analyzed, and adjusted, as necessary. The tool set consists of the following components:

- **Security Templates Snap-In.** This Microsoft Management Console (MMC) snap-in is a series of templates that allow you to create, edit, and save security configurations that can then be used to secure a local computer. It can also be imported into the Group Policy to be applied to all Windows 2000 machines within the Active Directory. This template can also be imported into the Security Configuration and Analysis Snap-In as the base configuration for security analysis. The Security Templates vastly improve configuration issues experienced with Windows NT. For example, all existing security attributes are in one place to ease security administration.

- **Security Configuration and Analysis Snap-In.** This MMC snap-in is used to analyze and configure local system security. This tool allows you import security templates and other security configurations to create scenarios and test them against the current system configuration. It is then possible to apply the settings to the current system using this tool. This tool is convenient when configuring individual machines and verifying security compliance with the Group Policy.

- **Security Settings Extension to the Group Policy Editor.** This tool allows the administrator to export the security configurations into a format that can be imported into the Group Policy. The administrator can use this tool to apply the entire security policy to all machines within the Active Directory. The Security Configuration engine will resolve any conflicts with the domain-level and local security policies using the precedence rules established by the Group Policy.

- **Secedit.exe command-line tool**. This command line tool allows the administrator to perform many of the configuration and analysis functions that can be achieved in the Security Configuration and Analysis Snap-in. This tool has the same analyze and configuration capabilities as the Security Configuration and Analysis tools, but it is intended for automated operations such as batch files and scripts. You can perform the security analysis from the

command line; but you cannot view the results with this tool. In order to view the results, the user must use the Security Configuration and Analysis Snap-in.

The two tools, Security Templates and Security Configuration and Analysis, are extremely useful for applying network security policy and evaluating whether individual machines are in compliance with the set security policy. With these two tools, you can build templates with particular security settings for different groups of machines, apply the settings to the machines, and then periodically evaluate the machines to verify that these machines remain properly configured.

The tools within the Security Configuration Tool Set all reply on each other as indicated in Figure 1 below:

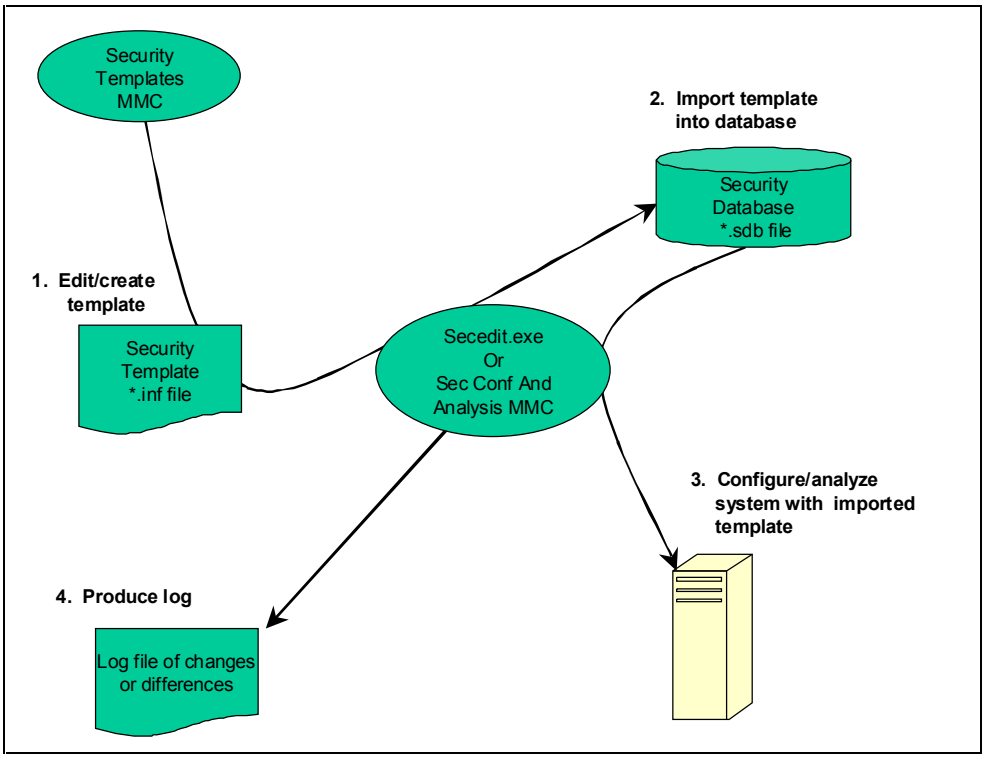

Figure 1: Security Configuration Tool Set

In a nutshell, the administrator starts with a security template (either a new one or edits an existing one). Next, he imports this security template into the database using the Security Configuration and Analysis Snap-in or Secedit.exe command-line tool. Then, using either of the Security Configuration and Analysis Snap-in or Secedit.exe command-line tool, the administrator can compare the local security settings against the template in the database. Finally, using the Security Configuration and Analysis Snap-in, the administrator can view the analysis and apply any found discrepancies to the local machine.

1.1 Security Templates Snap-In

Administrators can use the MMC Security Templates snap-in to build different security templates to either import into Group Policies or Local Security Policies. Administrators can either create a new policy from scratch or modify one of the dozen or so built-in security policies. These templates define Microsoft's recommended security settings to cover common levels of security. For example, the templates are defined for basic, compatible, secure, highly secure, and dedicated domain controller configurations.

After the administrator decides which template to use, he can import the template settings into the Group Policy Object (GPO) using Group Policy Editor (GPE) by right-clicking Computer Configuration, Windows Settings, Security Settings and choosing Import Policy. This process applies all the security settings configured in the template to any computer or user accounts in the site, domain, or organizational unit that he links the Group Policy to. The Local Group Policy is a special Group Policy object: it cannot override domain-based policy, and only local and account policies are part of the local security template settings. An example of the Security Templates Snap-In can be seen

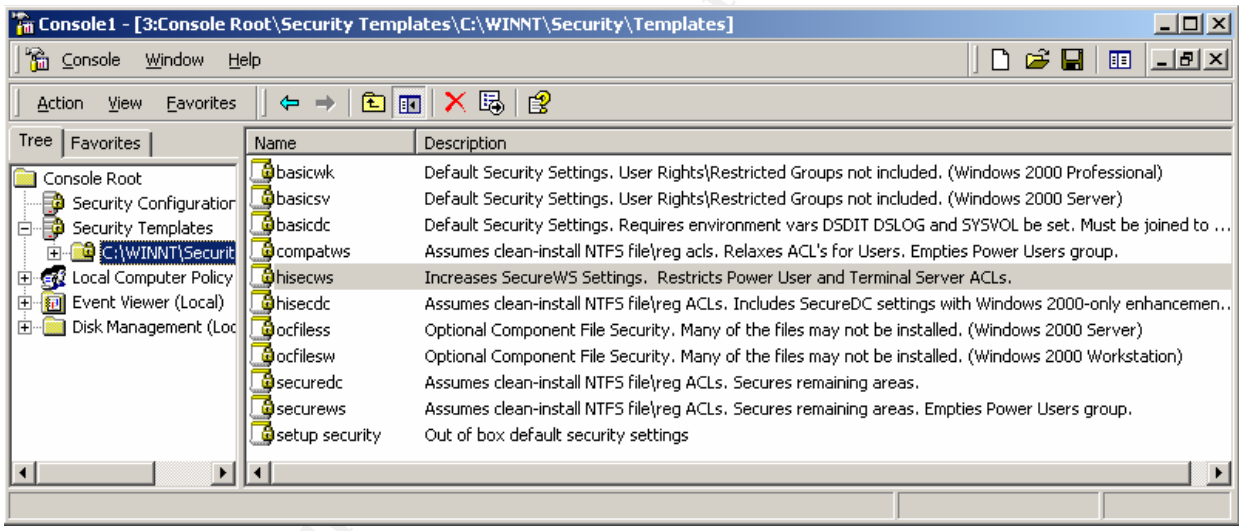

Figure 2: Security Templates

in Figure 2.

The idea of having a template to work from is a good idea. However, sometimes you may want to create a custom template based on your existing security structure rather than having to build the template completely from scratch.

1.1.1 Account Policies

The Account Polices folder defines the password settings, account lockout settings, and Kerberos settings. The password and account lockout settings are both items that were configured in Windows NT using the User Manager for Domains. Kerberos is a new type of authentication available for the first time in Windows 2000.

1.1.1.1 Password Policy

The Password Policy folder includes the security policy for passwords. In Windows NT, this was configurable in the Account Policy under User Manager for Domains. Figure 3 shows the present template for configuring the password security policy.

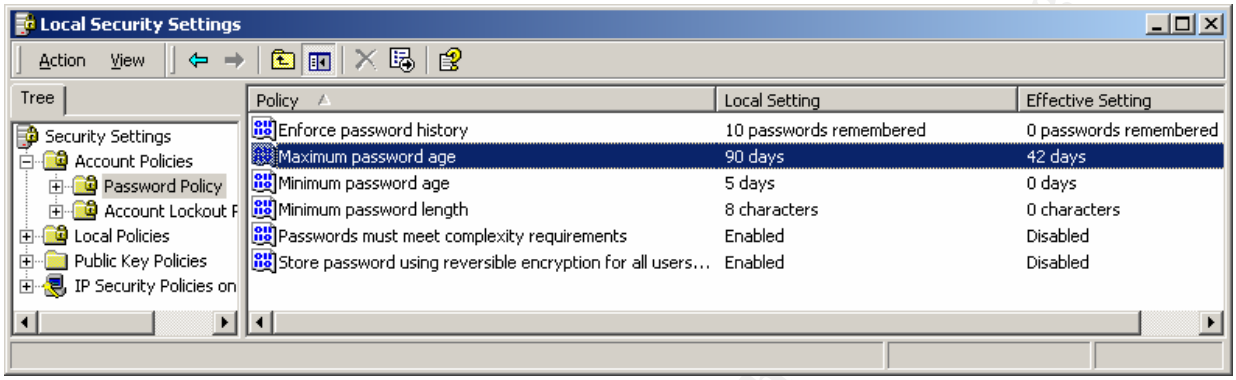

Figure 3: Password Policy Folder

Following is an explanation and recommended settings for the Password Policy settings:

- Enforce password history determines how many passwords will be remembered before the user can re-use the password. This setting is used in conjunction with the "Minimum password age" setting. This value should be set to keep a history of 8 to 13 passwords. *(Windows NT/2000 feature)*

- Maximum password age determines how long a user can keep the same password before it must be changed. This value should be 45 to 90 days. *(Windows NT/2000 feature)*

- Minimum password age determines how long a user must keep a password before they change it. This setting prevents users from cycling through old passwords. It is used in conjunction with the Enforce Password History setting. This value should be set between 1 and 5 days. *(Windows NT/2000 feature)*

- Minimum password length determines the minimum characters acceptable for a password. This value should be set to at least eight characters. *(Windows NT/2000 feature)*

- Passwords must meet complexity requirements determines the types of characters required in a password. The complexity depends on the applied password filter. For example, if the passfilt.dll is used, passwords must be at least six characters long, cannot contain the user name, and must use three of the four available character types (i.e., lowercase letters, uppercase letters,

numbers and symbols). *(This feature was only configurable using the registry in Windows NT.)*

- Store password using reversible encryption for all users in the domain allows passwords to be recovered in case of an emergency. Forgetting a password is not an emergency situation because any administrator can go in and change the user password. *(This is a new feature in Windows 2000.)*

1.1.1.2 Account Lockout Policy

The Account Lockout Policy folder determines when and for whom an account will be locked out of the system. It consists of the following configurable security items: Account lockout duration, Account lockout threshold, and Reset account lockout counter after. Figure 4 shows these three attributes and how they are configured.

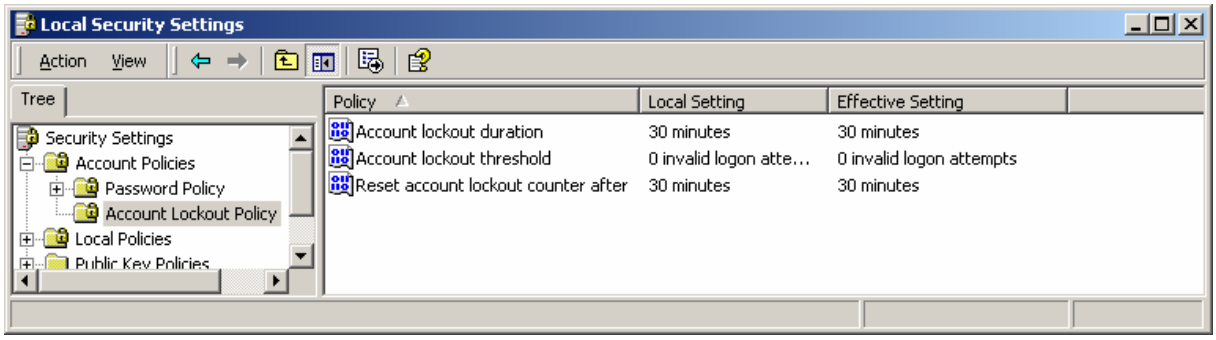

Figure 4: Account Lockout Policy Folder

1.1.1.3 Kerberos Policy

The Kerberos Policy folder only applies to domain controllers, since local logons do not use Kerberos. The policy settings include shown in Figure 5. An explanation of these attributes follows since this is a new feature in Windows 2000.

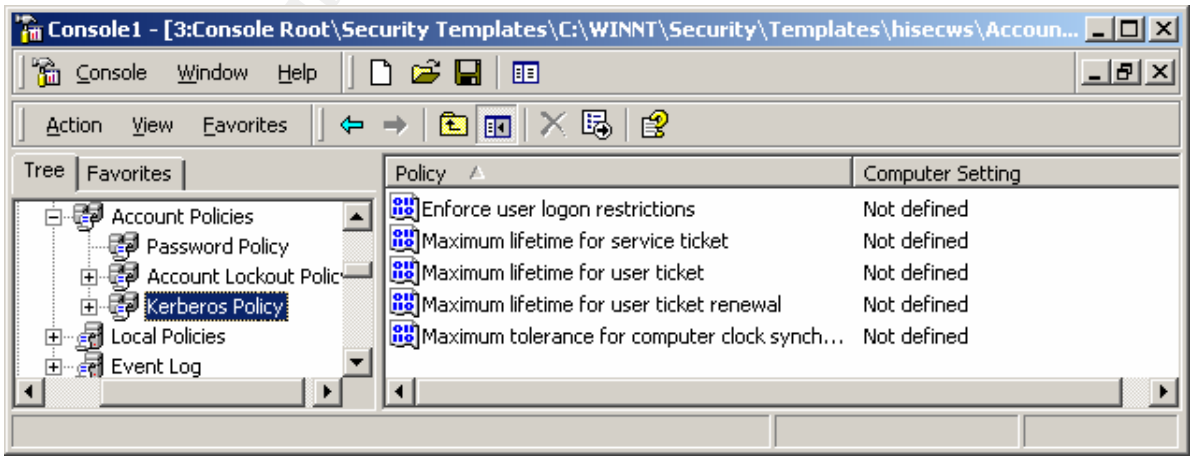

Figure 5: Kerberos Policy Folder

- Enforce user logon restrictions defines the target computer's user right policy. This process can slow down network access. This attribute can either be set to enabled or disabled. Disabling this setting can speed up the access to the network service, but it is less secure.

- Maximum lifetime for a service ticket defines how long a user can access a service with a given session ticket.

- Maximum lifetime for a user ticket defines how long a user can use the ticket-granting ticket (TGT) before renewing it or requesting a new one. *(The TGT is used by the client to request session tickets.)*

- Maximum lifetime for a user ticket renewal determines the length of time a continuously renewed TGT is valid.

- Maximum tolerance for computer clock synchronization defines the allowable difference between the client's and server's clock.

1.1.2 Local Policies

Local policies only apply to the local machine. This folder consists of the Audit Policy, User Rights Assignment, and the Security Options. Whereas the Security Template includes the security settings for the Audit Policy, User Rights Assignment, and the Security Options, Windows NT required two programs. NT required the User Manager for Domains for the Audit Policy and the User Rights Assignment, and the Security Options settings had to be directly manipulated using the registry for Windows NT. The Security Templates made configuring these three categories much simpler for the administrators.

1.1.2.1 Audit Policy

The user's actions must be audited and these settings for controlling what will be audited are included in the Security Templates. The most basic form of intrusion detection is to enable auditing. This will alert the administrator to changes in account policies, attempted password hacks, unauthorized file access, etc. Most users are unaware of the types of doors they have unknowingly left open on their local workstation, and these risks are often discovered only after a serious security breach has occurred. At the very minimum, the administrator should consider auditing the following events shown in Figure 6.

1.1.2.2 User Rights Assignment

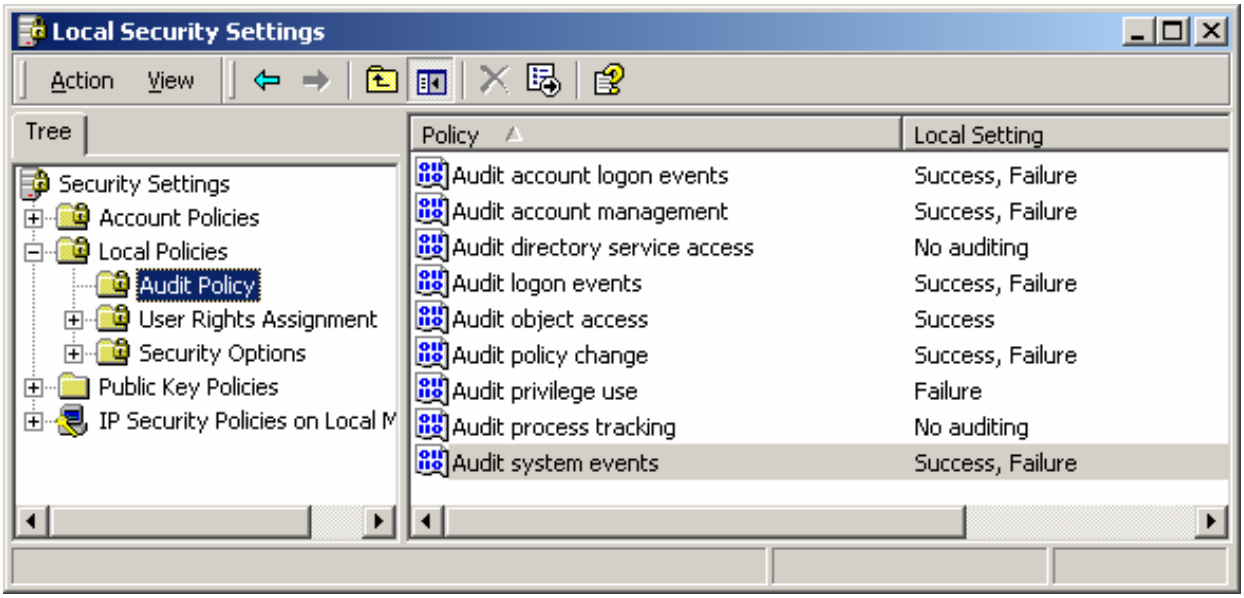

Figure 6: Audit Policy Folder

The configuration of user rights is much easier in Windows 2000 than previously in Windows NT. In Windows NT, user rights were configured through User Manager for Domains. It was quite tedious to configure the individual user rights because only one right was viewable at a time. This also made it difficult to check the applied user rights settings unless a third party tool was used. All user rights are now easily configured with the Security Templates Snap-in as shown in Figure 7. The user right and the applied setting for all rights are viewable in one window.

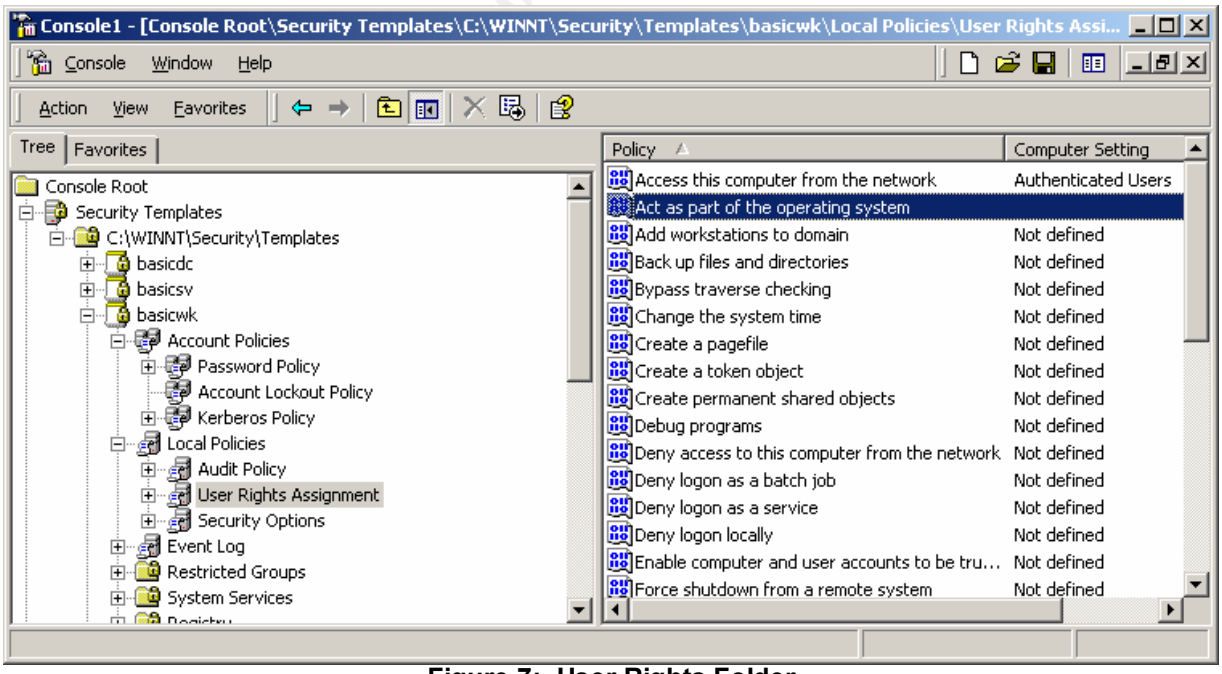

Figure 7: User Rights Folder

1.1.2.3 Security Options

The Security Options folder contains many items that were only configurable through the registry (regedt32.exe) in Windows NT. This folder has significantly reduced the time system administrators need to spend looking for and editing registry keys. An example of some of the settings can be seen in Figure 8. The Security Options include items such as allowing the system to be shutdown without logging in, restricting anonymous connections, requiring the CTRL+ALT+DEL sequence for logon, and the time period in which to prompt the user before password expiration. All of the Security Options are easily edited in Security Tool Set verses the manual intensive process experienced with Windows NT.

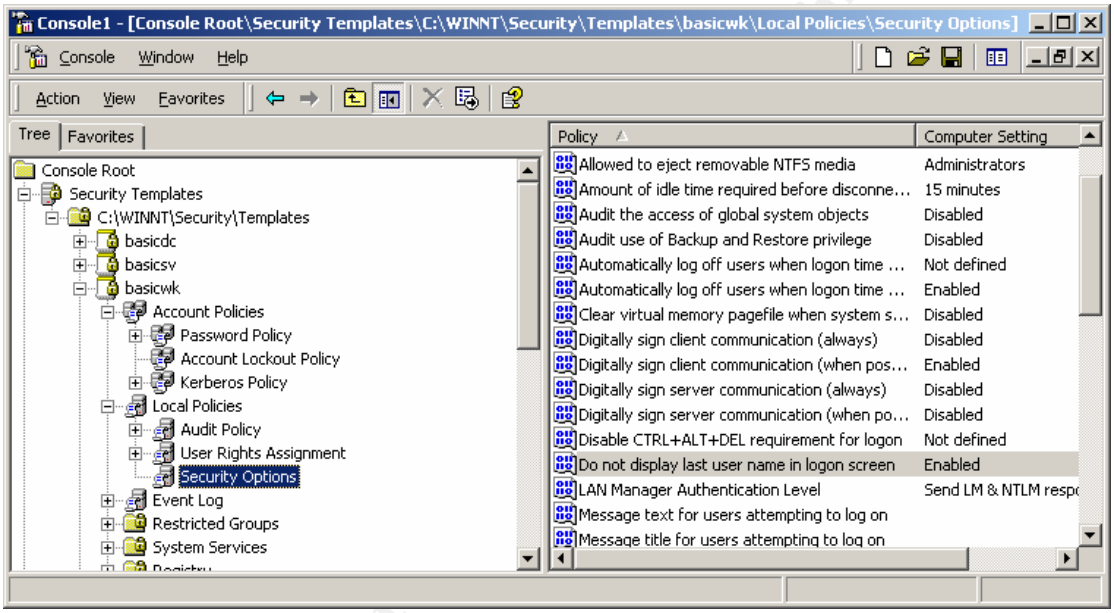

Figure 6: Security Options Folder

The predefined list of registry keys listed in the Security Templates may not be complete for every organization. The Security Options folder can be extended to support additional registry settings. The Security Options entries for the Security Configuration Tool Set are stored in the registry under the following key:

HKLM\Software\Microsoft\WindowsNT\CurrentVersion\SeCEdit\Reg Values

where “Reg Values” represents the mapping to the registry value where the values are actually set. For example, the name for the registry subkey

HKLM\System\CurrentControSet\Services\EventLog\System\RestrictGuestAccess
is
MACHINE/System/CurrentControSet/Services/EventLog/System/RestrictGuestAccess

1.1.3 Event Log

In Windows 2000, the Event Log folder consolidates the event log security settings into one place. In Windows NT, these settings were set in both the registry and the User Manager for Domains. Multiple windows needed to be opened to view the current settings. Windows 2000 has eliminated this tedious process and made all event log settings available in one window as indicated in Figure 9. These settings include maximum log sizes, configuring guest access to the logs, length of log retention, and whether or not to shutdown the computer when the security log is full.

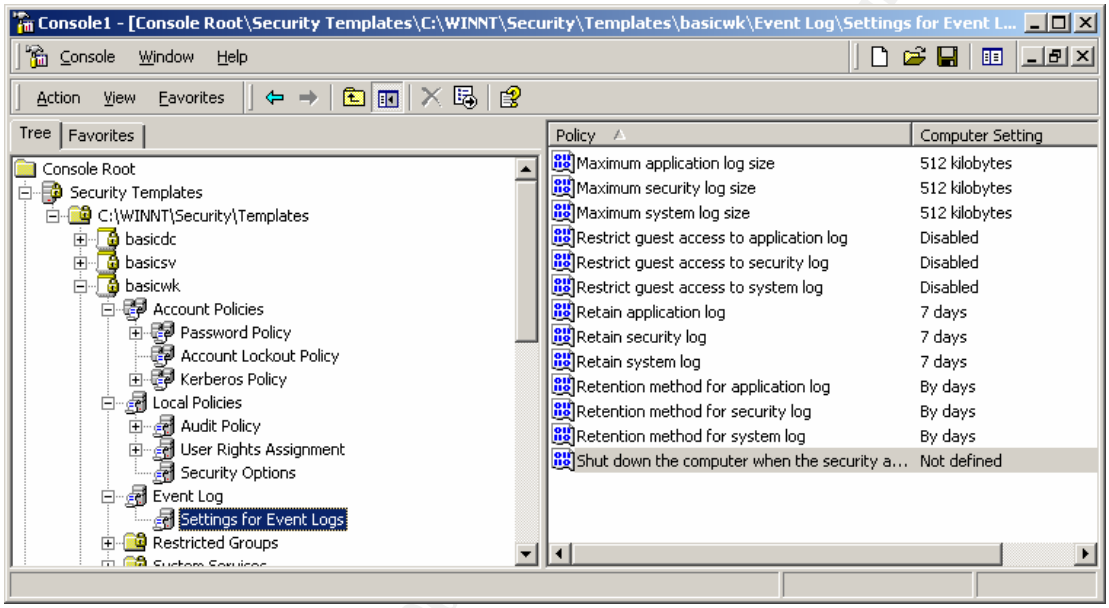

Figure 7: Event Log Folder

The event log files can grow very rapidly so administrators should closely monitor the log files and allocate sufficient space for reasonable log accumulation. For the best security, the security policy should be configured to not overwrite events automatically. These log files are stored in the winnt\system32\config directory. Administrators need to monitor these files for a few days to determine how large to set the maximum size for the logs.

1.1.4 Restricted Groups

The Restricted Groups is a new security feature in Windows 2000 that allows the administrator to centrally control the members of groups. At times, administrators temporarily need to add users to groups with more privileges than a typical user. For example, this might be the case when an administrator goes on vacation. Many times the administrator later forgets to remove the elevated privileges thus potentially creating a security hole. Figure 10 shows the Restricted Groups folder.

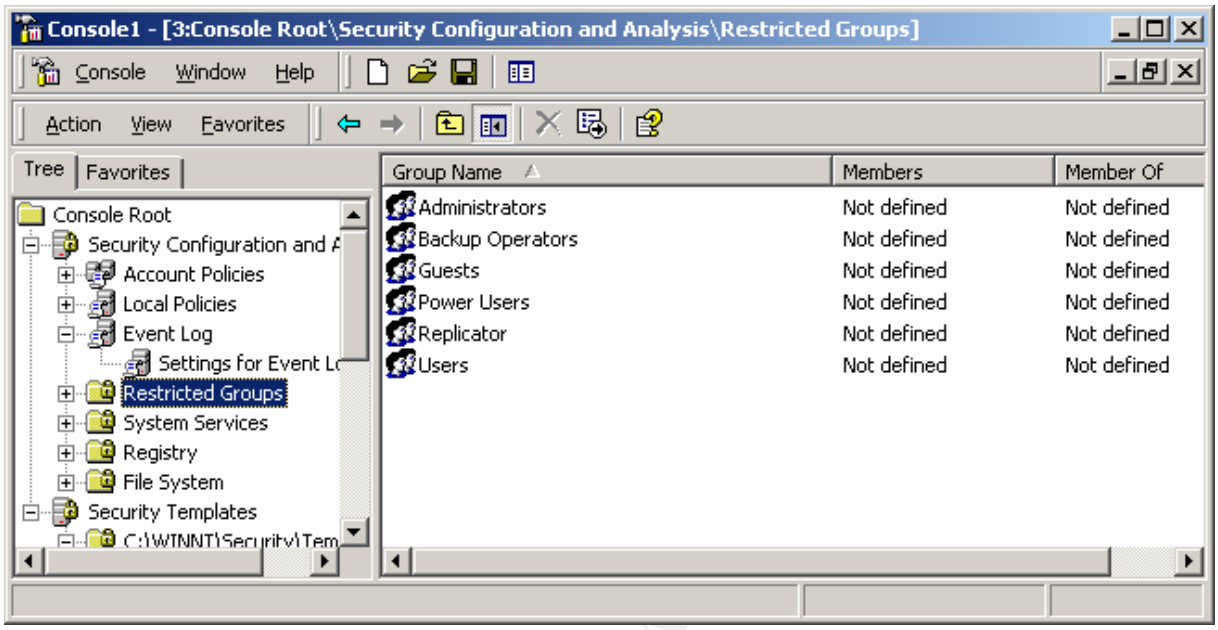

Figure 8: Restricted Groups Folder

1.1.5 System Services

The System Services folder allows the administrator to define whether a service startup should be automatic, manual, or disabled. The administrator can also control what user accounts have access to each service. This is extremely important because a large security hole could be created if a service such as FTP Publishing service were automatically started and anonymous connections were allowed.

In Windows NT, the administrator has to go into the Control Panel to configure startup services. Once again, the Security Template simplifies another process for the administrators. Figure 11 shows some of the controllable system services.

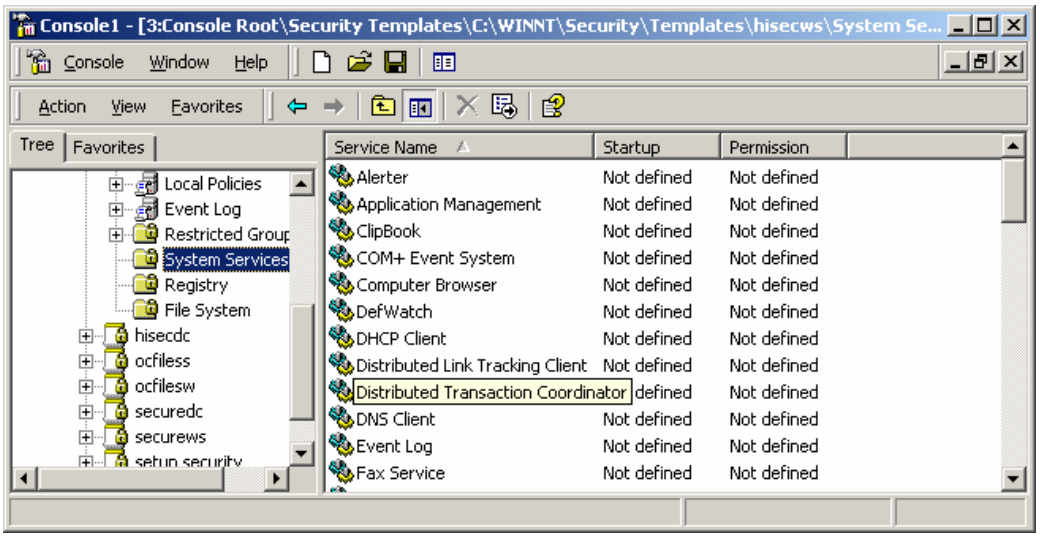

Figure 9: System Services Folder

1.1.6 Registry

Instead of using regedt32.exe as in Windows NT, the Security Template allows the administrator to set access-control permissions and audit settings for certain registry keys or value, and then customize how the settings propagate. Windows 2000 has made this task much easier and less error-prone. Figure 12 shows entries in the registry folder that can be configured.

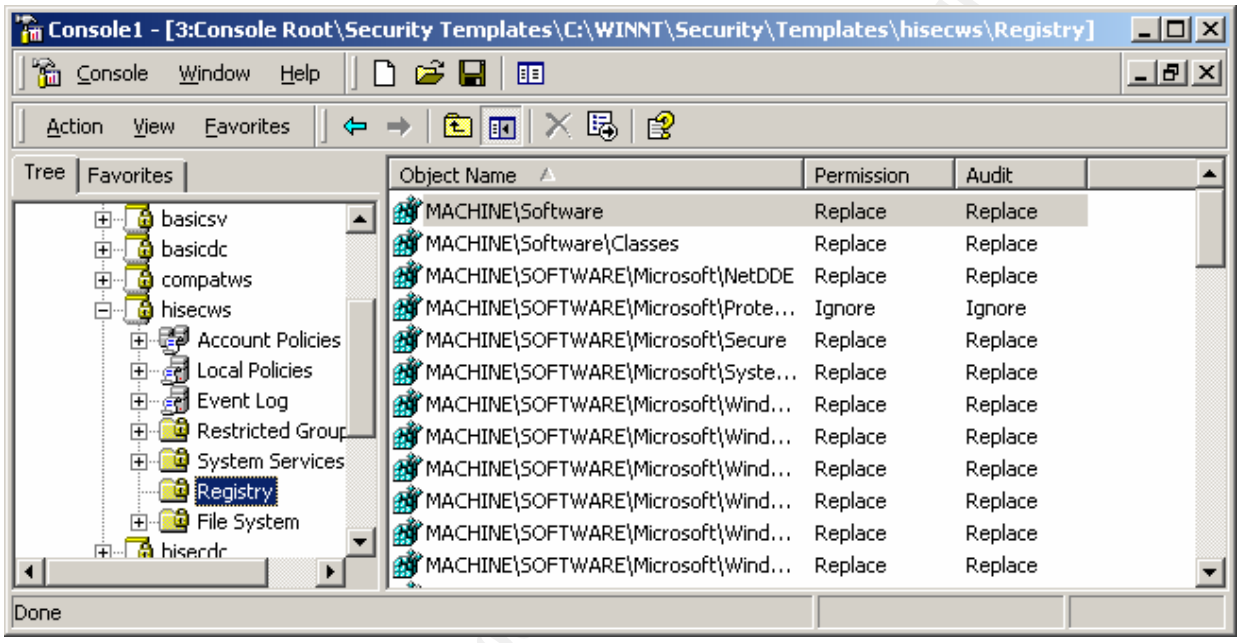

Figure 10: Registry Folder

Figure 13 shows how the security policy settings could be configured to for an individual registry key.

Figure 11: Configuring Registry Key

1.1.7 File System

Finally, the File System folder allows the administrator to configure NTFS permissions for users of all local drives, folders and files. Some of the directories can be seen in Figure 14.

In the Security Templates, the specific drive letters are not specified. Administrators can assign drive letters by right-clicking on the File System folder and selecting “Add File”.

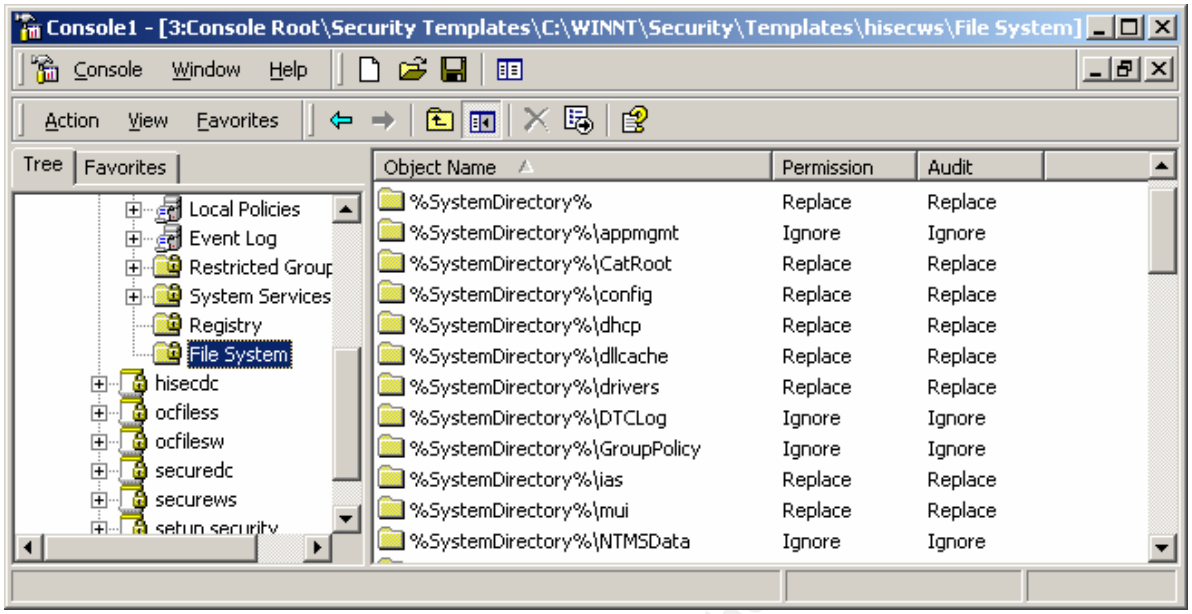

Figure 12: File System Folder

This tool is a great aid to the administrator who needs to change the access permissions on a large number of files or folders and later cannot remember what the original settings were. A security template could be applied to restore all the original permissions back to the files or folders.

1.2 Security Configuration and Analysis Snap-In

The Security Configuration and Analysis Snap-in is one of the most useful tools in the Security Configuration Tool Set. This tool gives the administrator the ability to easily compare the desired security settings from a template to the actual state of the local machine. This verifies that the security settings administrators apply with the Group Policy are effective.

Before a security analysis can be performed a database must be created to store the results. After the database is created, the template containing the security settings to be applied to a specific machine needs to be added to the database. Once this is done, a screen similar to Figure 15 will appear. It contains all the instructions needed to both analyze and configure the local machine.

To start the analysis, simply right-click the snap-in and choose Analyze Computer Now. This will check the actual security settings on the local computer against the desired settings. The machine will run the analysis and display its progress, as shown in Figure 16. After the program is finished analyzing the local machine. The administrator can view the results.

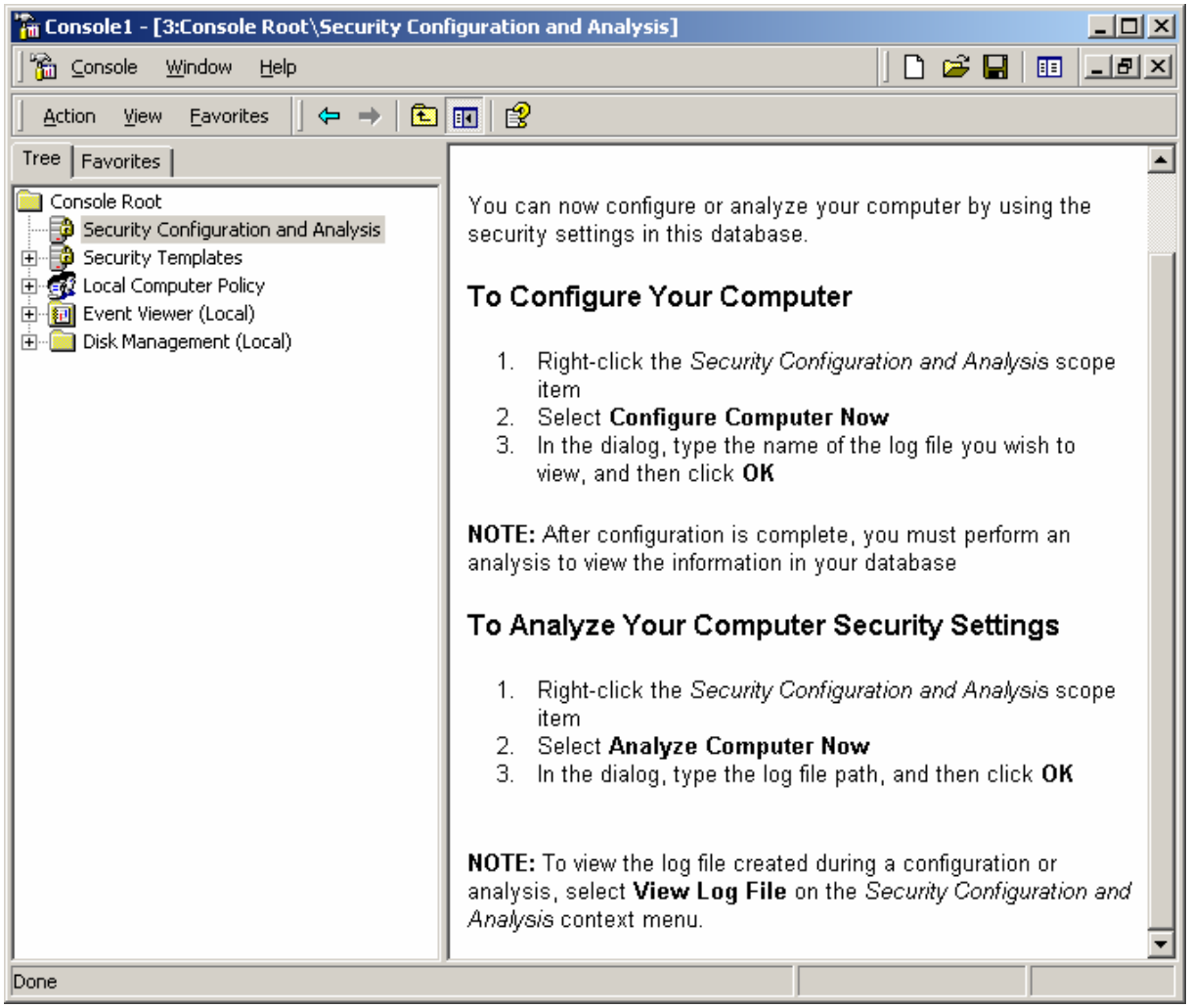

Figure 15: Configuration and Analysis Window

The administrator can also use Security Configuration and Analysis to apply the security template to the machine, but it's better to use Group Policy. If you use Security Configuration and Analysis to apply the settings, a user can come behind the administrator and change the settings. With Group Policy, if a user changes a security setting, it changes back to its original value the next time Windows 2000 replicates the security policy.

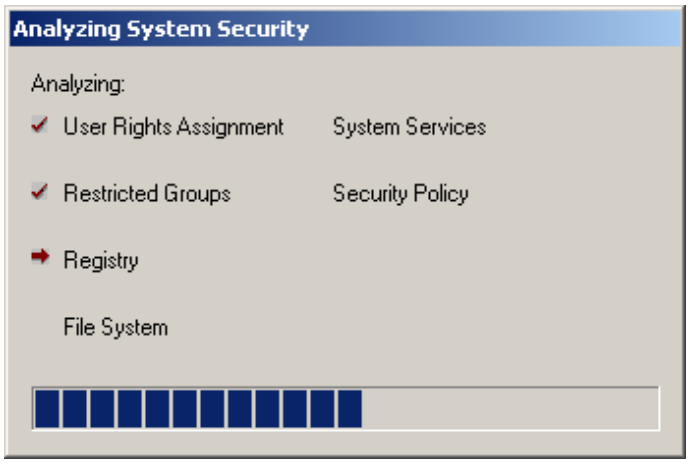

Figure 16: Analysis Progress

It is a good idea to use the Security Configuration and Analysis Tool before applying the new Security Template to the Group Policy. The reason for this is the administrator may want to keep an existing setting instead of overwriting it with the recommended template setting. For example, suppose the Administrator's account has stricter permissions applied to it. He wouldn't want to blindly apply a security template to reduce the security level of this particular account.

1.2.1 Analyzing the Results

After the snap-in analyzes the differences between the computer security settings and the selected security template settings, it is time to review the results in each folder. Not all discrepancies are reported the same. The following paragraphs explain what to look for in the results.

1.2.1.1 Account and Local Polices Analysis

Figure 17 is an example of what a typical analysis screen looks like for Account and Local Policies. The icons with green checks indicate that the database settings and the local machine settings are the same. Icons with a red "x" indicate that there is a discrepancy between the database and the local machine settings. Icons with neither a checkmark nor an "x" indicate that no setting was present in the database. In Figure 17 only two of the six computer settings actually match the settings in the database.

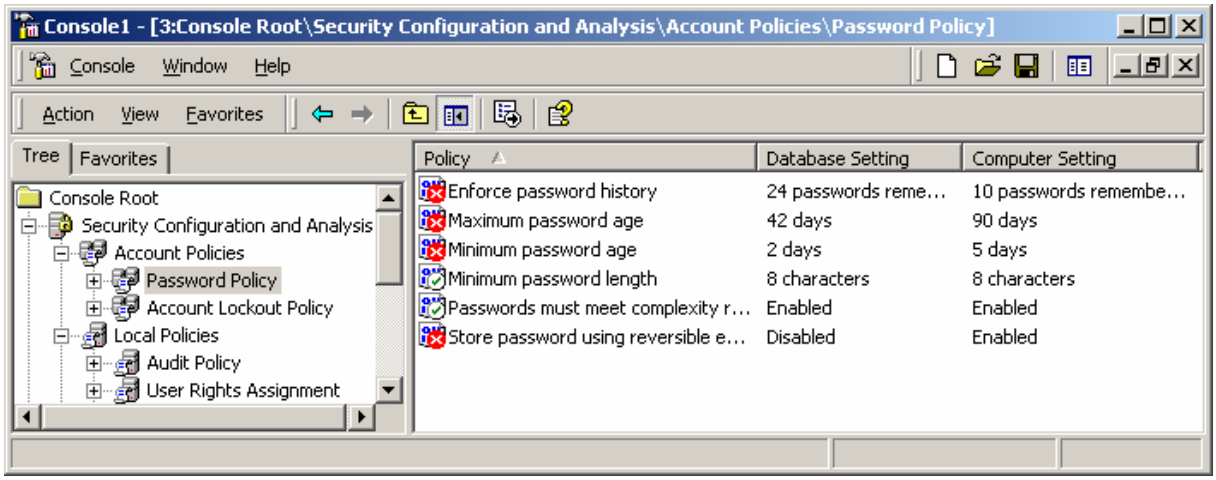

Figure 17: Password Policy Analysis

1.2.1.2 Restricted Group Analysis

Figure 18 shows the results of the Restricted Group analysis. The columns, Members and Members of, show an OK status. The same icons that applied to the Account Policy also apply to the Restricted Groups.

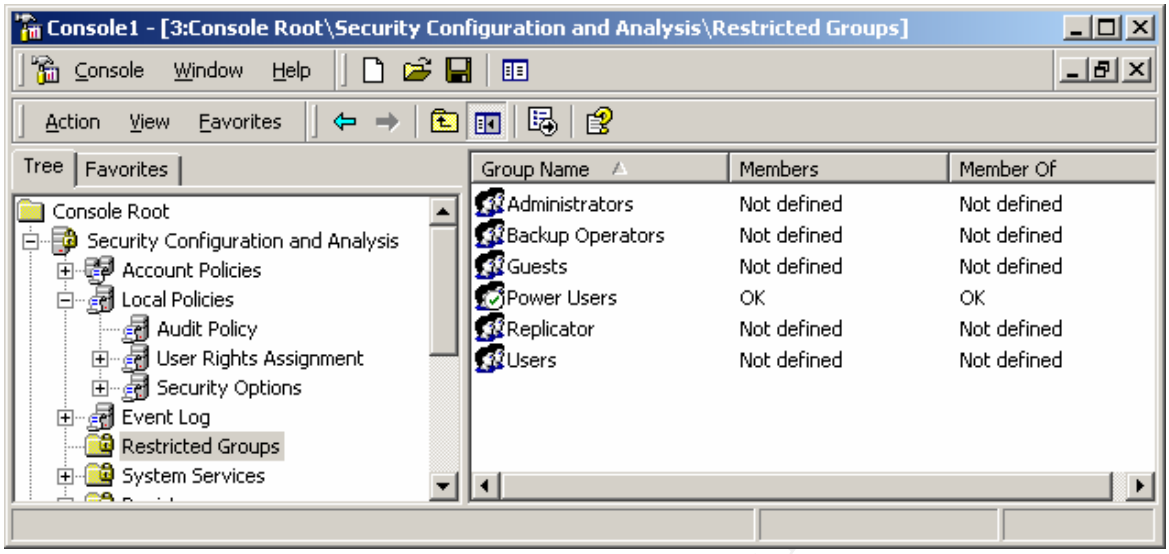

Figure 18: Restricted Group Analysis

1.2.1.3 Registry Analysis

Figure 19 shows the results of the Registry analysis. If registry items were not defined in either the database or the applied security policy, it is indicated by the text "Not defined". If the text "Subitems defined" appears, as in Figure 19, the administrator needs to traverse down the registry keys to find the actual discrepancy.

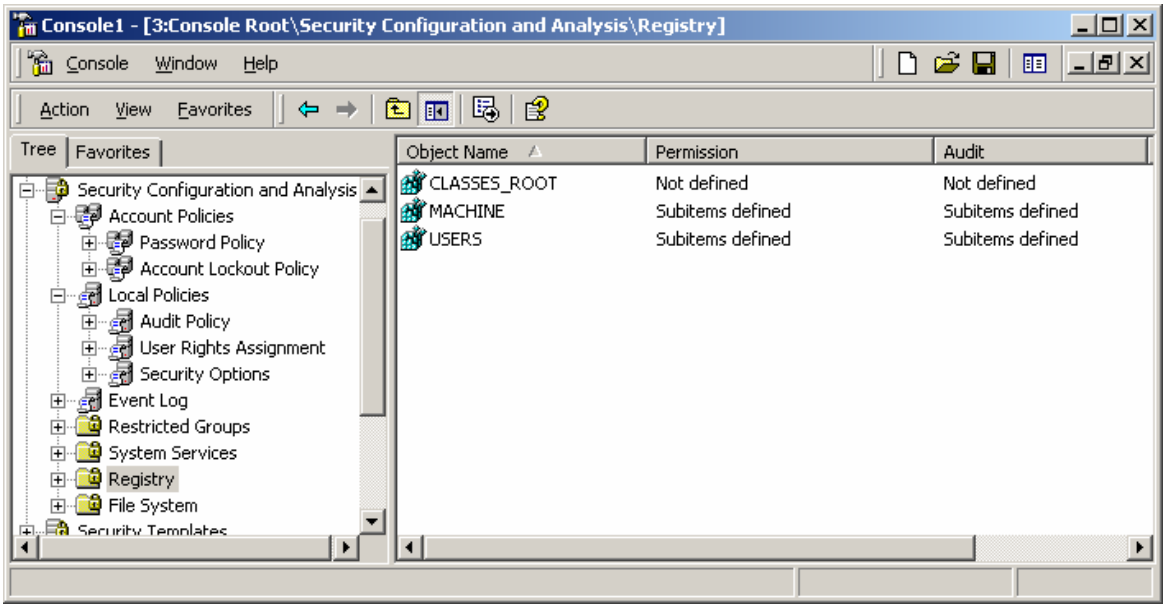

Figure 19: Registry Analysis

1.2.1.4 File System Analysis

Figure 20 shows the results of the File System Analysis. Drive D:\ is configured according to the database but there are discrepancies in the C:\ and E:\ drives that need to be investigated.

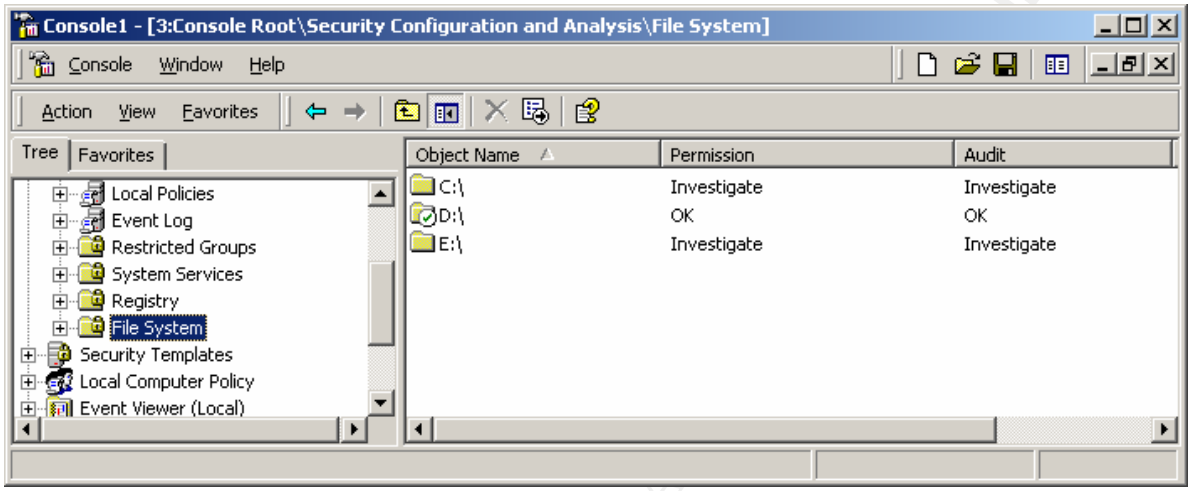

Figure 20: File System Analysis

1.2.1.5 System Services Analysis

Figure 21 shows the results of the System Services analysis. Again, the green checkmarks for are used for to indicate local security settings that are identical to the database settings.

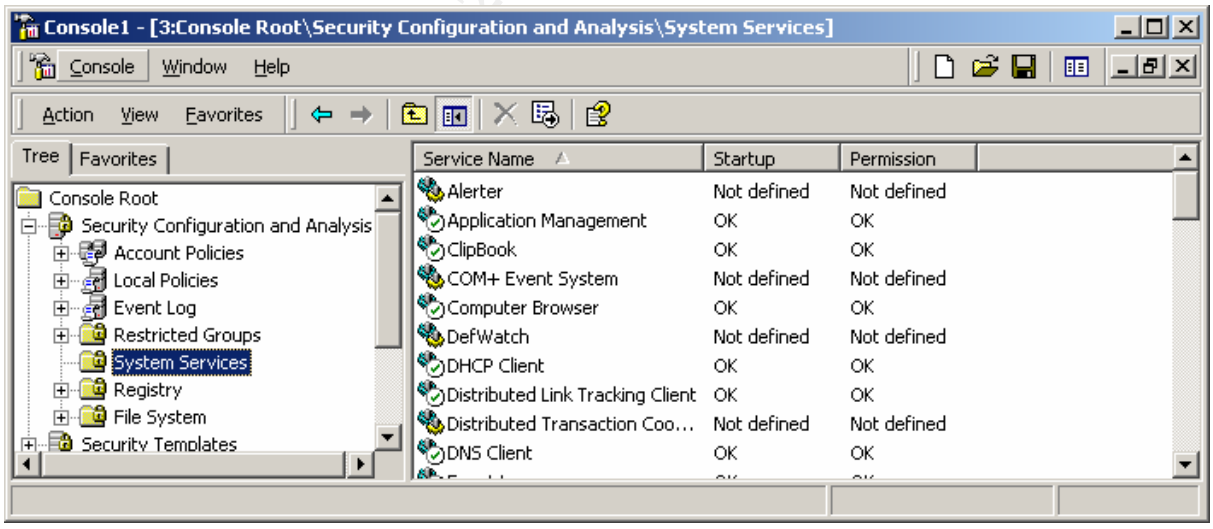

Figure 21: System Services Analysis

1.2.2 Configuring the Computer

Once the results for the security analysis have been reviewed, the administrator can either apply the database settings to the local computer or update the database settings to match the local machine. To update the database, the administrator simply right-clicks on the object, selects "Security", and makes the appropriate change. Figure 22 shows this being done for the "Enforce Password History Policy".

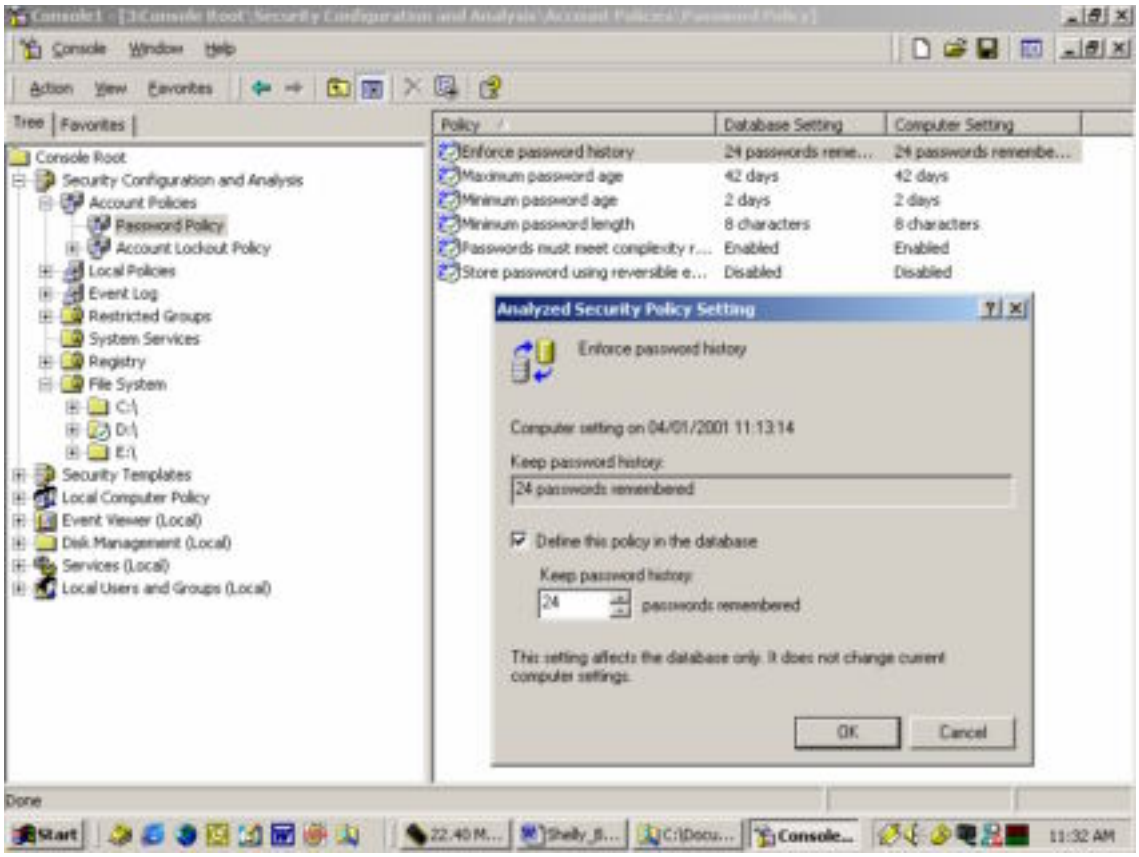

Figure 22: Updating the Database

If the administrator wishes to update the local computer to include all the database settings, he will right-click on Security Configuration and Analysis and select "Configure Computer Now" as shown in Figure 23. All of the security settings on the local machine will be changed to match the current database settings. Be advised that this is a permanent change: there is no undo action.

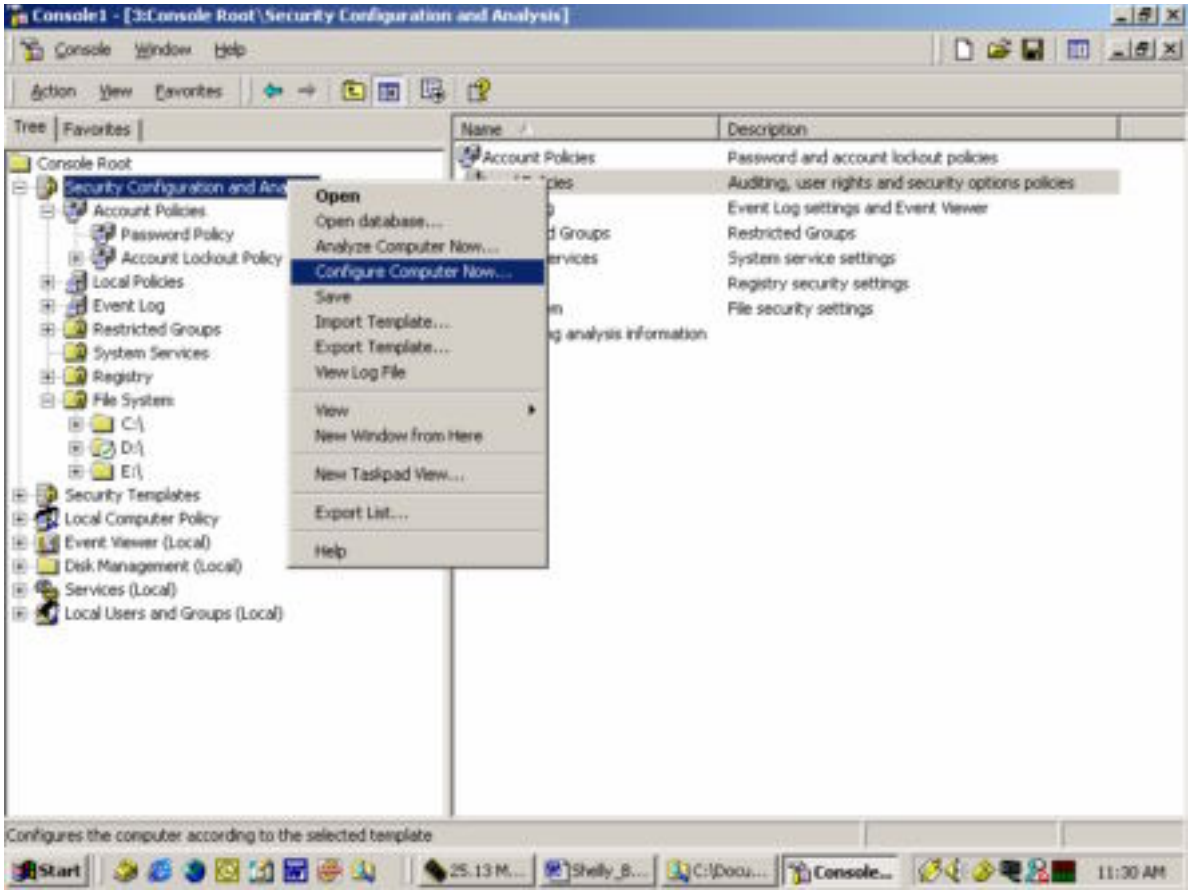

Figure 23: Configuring the Local Machine

1.3 Security Settings Extension to the Group Policy Editor

Whereas the Security Configuration and Analysis Snap-in allows the administrator to easily configure local security policies, the Security Settings Extension to the Group Policy Editor allows for the configuration of an entire organizational unit, domain, or site – or in other words, machines contained in the Active Directory. The Group Policy is the successor to the System Policy Editor present in Windows NT.

Applying a security template to the entire domain or organizational unit is an easy task in Windows 2000. The administrator simply creates a new Group Policy by opening up the Active Directory User and Computer console from the Administrative Tools menu. From here right-click an organizational unit and select Properties. Click the button New and type a name for the Group Policy Object. Select the new object and then click the button Edit. Figure 24 shows the Group Policy Window. Next, expand the Computer Configuration folder. Right-click on the Security Settings folder and select Import Policy. Select the security template to import and then click open. The selected security template will be applied as soon as the file is imported and then replicated across the organizational unit or domain.

After applying a security template to an entire domain or organizational unit, conflicts between local security policy and domain-level policy arise. These conflicts are resolved by the Security Configuration Engine. Precedence ALWAYS falls with the Group Policy. The domain-security policies always override the local security policies. The local security policy may be set to automatically start the service Telnet while the Global Policy is set to disable the Telnet service on startup. The Global Policy, effective setting, will override the Local Policy, computer setting.

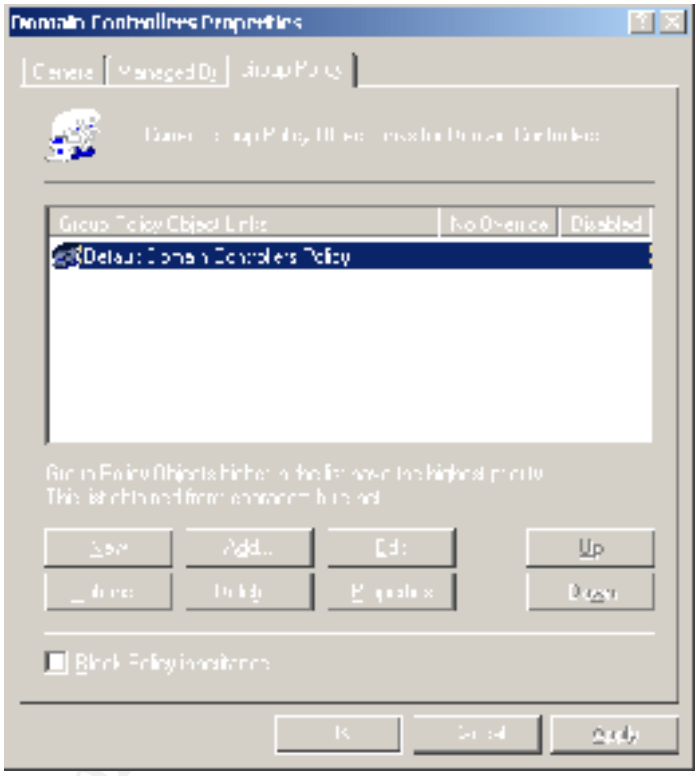

Figure 24: Group Policy GUI

1.4 Secedit.exe Command-line Tool

The Secedit.exe command-line tool, when called from a batch file or automatic task scheduler, can be used to automatically create and apply templates and analyze system security. It can also be run dynamically from a command line. This tool is useful when administrators have multiple computers on which security must be analyzed or configured, and need to perform these tasks during off-hours.

One advantage of the secedit.exe command-line tool is that it allows administrators to analyze a number of machines by creating scripted that can be automated. The results are then viewed by opening up the database file that the analysis was run against. However, one drawback is that the results from the analysis cannot be viewed from this tool. Viewing must be conducted from the Security Configuration and Analysis Snap-in.

2.0 Conclusion

The Security Configuration Tool Set has greatly reduced the costs associated with security administration. This paper demonstrate how centrally located all security settings are within Windows 2000. Through the use of the Security Configuration and Analysis Snap-in, security configuration components can now be effortlessly configured. This is a major breakthrough since Windows NT 4.0 where the security configuration items were spread throughout many different programs.

References

Global Knowledge Professional Reference. Configuring Windows 2000 Server Security, Syngress Media. 2000.

Fossen, Jason, "*Securing Windows NT: Step-by-Step*, version 3.6", The SANS Institute, 24 July 2000.

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

Schultz, E. Eugene. Windows NT/2000 Network Security, McMillan Technical Publishing, 2000.

Microsoft Press, Microsoft Windows 2000 Security Technical Reference, 2000.

National Security Agency. *"Guide to Securing Microsoft Windows NT Networks"*. September 6, 2000.

Last Updated: October 19th, 2017

Upcoming Training

San Francisco Winter 2017 - SEC505: Securing Windows and PowerShell Automation	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**vLive**
SANS San Francisco Winter 2017	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**Live Event**
SANS Cyber Defense Initiative 2017	**Washington, DC**	**Dec 12, 2017 - Dec 19, 2017**	**Live Event**
Univ. of California - SEC505: Securing Windows and PowerShell Automation	**Los Angeles, CA**	**Jan 29, 2018 - Feb 03, 2018**	**vLive**
SANS Southern California- Anaheim 2018	**Anaheim, CA**	**Feb 12, 2018 - Feb 17, 2018**	**Live Event**
Southern California- Anaheim 2018 - SEC505: Securing Windows and PowerShell Automation	**Anaheim, CA**	**Feb 12, 2018 - Feb 17, 2018**	**vLive**
SANS 2018	**Orlando, FL**	**Apr 03, 2018 - Apr 10, 2018**	**Live Event**
SANS Security West 2018	**San Diego, CA**	**May 11, 2018 - May 18, 2018**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**