# Global Information Assurance Certification Paper

## Copyright SANS Institute
## Author Retains Full Rights

GIAC Certified Windows Security Administrator (GCWN) Practical
Assignment
V3.1



Using Windows 2000 Security Templates to create a Secure
Web Monitoring Server

Submitted by Brad P. Towers    *CISSP*
GCWN Practical Assignment, version 3.1
Date submitted: April 07, 2003

# **Table of Contents:**

**1.0 Introduction**

Microsoft Windows, as an Operating System, has its roots as what I like to call a "Business Enabler". Windows was designed to make information sharing as well as access to needed information and programs as simple as possible. From a business perspective, this makes good sense, however it becomes a different story when we are looking at it from an Information Security viewpoint. The fact that access to information, services, and programs is relatively easy to access is both a feature and a bane at the same time. This practical discusses the selection and application of an existing Windows 2000 Security Template applied to a server for testing, before being put into production. The Windows 2000 based system I will be using, will be performing the role of a Web Content filtering server. The logical placement of this Web Content server will be directly in front of my outbound Microsoft ISA Server running in Web Proxy mode. In addition to it's role as a content filtering server, the server in question will be running Windows Terminal Server in remote administration mode.

Microsoft has made it easier to set up and manage the security settings for an organization's network, as Windows 2000 Server includes the Security Templates tool. The Security Templates tool is a Microsoft Management Console (MMC) snap-in that allows administrators to define standard templates and apply them equally to multiple computers or users. In this practical, I will be applying a template (W2K_Server.INF) that has been created by the National Security Agency (NSA) for Windows 2000 Server. Although Microsoft supplies several "role based" templates with the Windows 2000 Server, I opted to select a Template that was created and verified by an independent organization. In fact, the templates supplied by the NSA are a collaboration of several government agencies.

After the template has been applied, I will begin testing and documenting my test results. Any changes made to the Template as a result of my testing will be documented, as well as my reasoning for the alterations.

**1.1 Security Template Definition and Uses**

A security template is a physical representation of a security configuration; what this means is there is a text file where groups of security settings are stored. These settings could be edited through a simple text editor, such as word-pad or notepad. However, the Security Templates tool described above is the preferred method for modifying Security Templates. A Security Template is one component that makes up a Group Policy Object (GPO). A GPO is in fact made up of a Group Policy Template (Security Template) and a Group Policy Container, which is stored in Active Directory. Windows 2000 includes a set of standard security templates, each appropriate to the role of a particular computer. The templates range from security settings for low security domain clients to highly secure

domain controllers. These templates can be used as provided, modified, or serve as a basis for creating custom security templates.

Also included with Windows 2000 is the Security Configuration and Analysis tool. This can be used to apply the restrictions defined in a security template to actual systems. It can also be used to analyze a system's security and to compare the settings on computers that have been deployed to make sure they conform to company standards.

Below are several screenshots that show the Security Templates, both in the Security Template Tool within the MMC, and the Text version of the same Template.
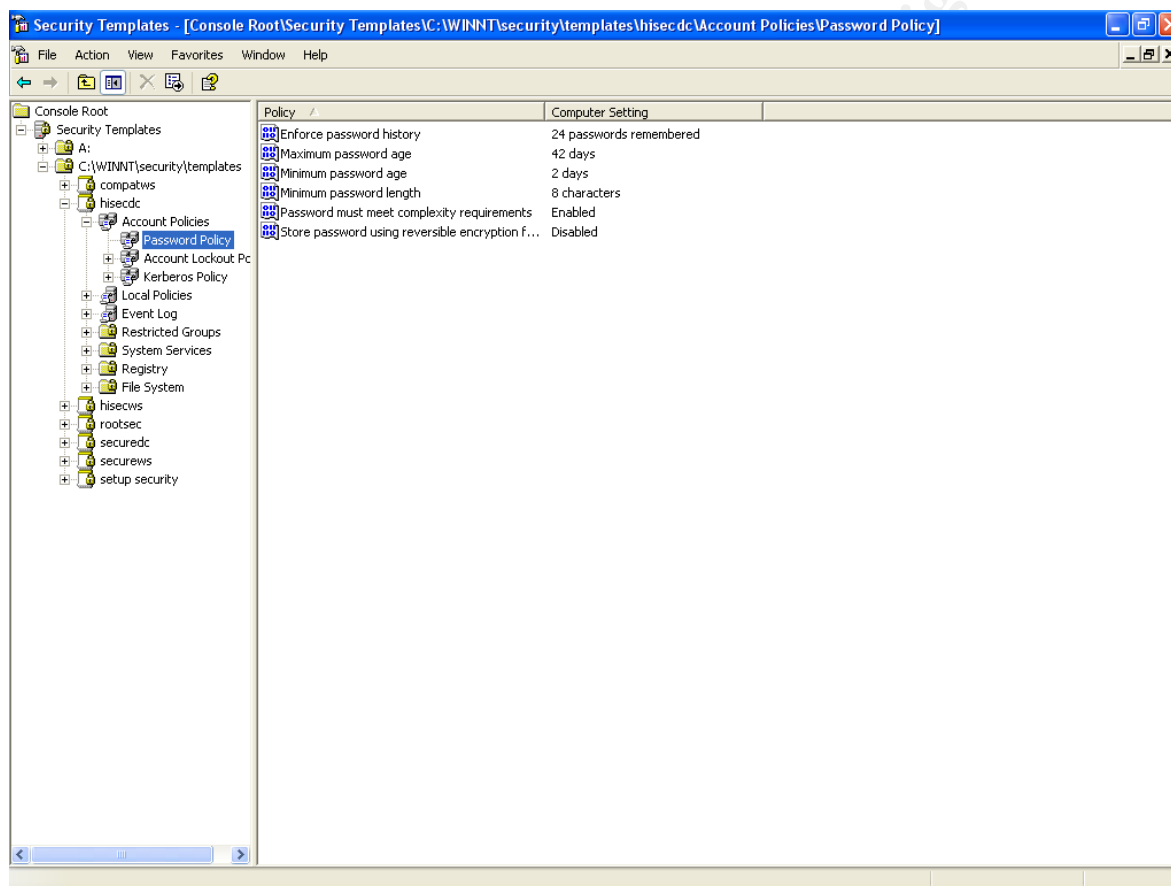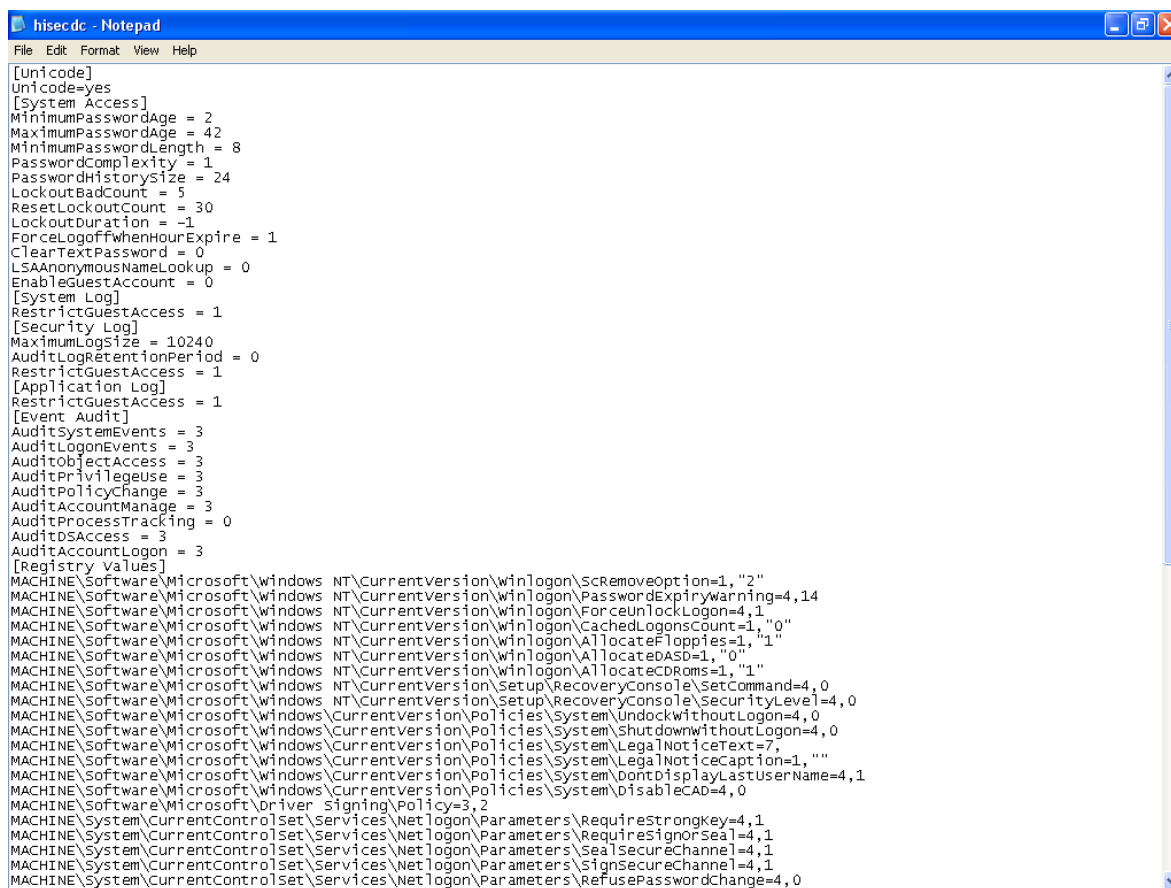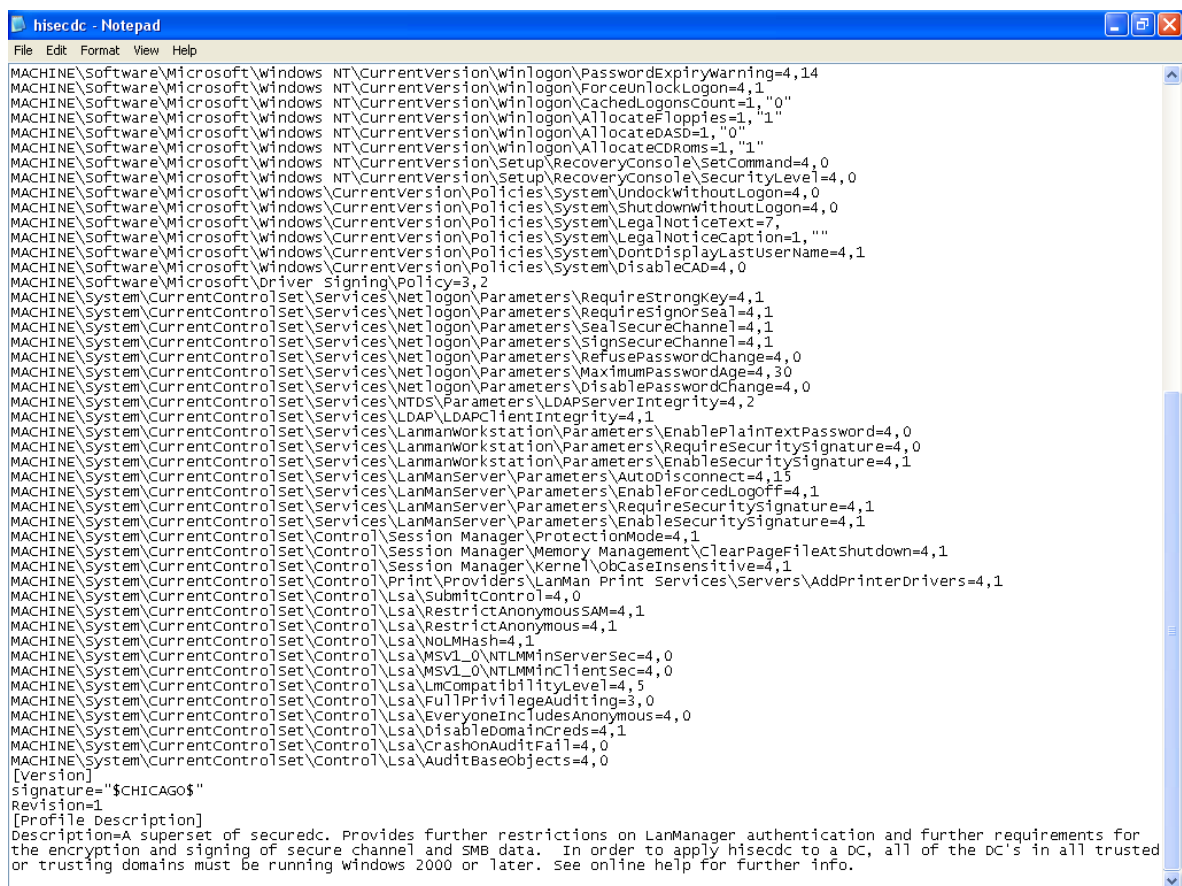


**Figure 1- MMC Security Template Example**

Now, here is the same policy, only this is the text only representation of the this policy.

```
hisecdc - Notepad
File  Edit  Format  View  Help

[Unicode]
Unicode=yes
[System Access]
MinimumPasswordAge = 2
MaximumPasswordAge = 42
MinimumPasswordLength = 8
PasswordComplexity = 1
PasswordHistorySize = 24
LockoutBadCount = 5
ResetLockoutCount = 30
LockoutDuration = -1
ForceLogoffwhenHourExpire = 1
ClearTextPassword = 0
LSAAnonymousNameLookup = 0
EnableGuestAccount = 0
[System Log]
RestrictGuestAccess = 1
[Security Log]
MaximumLogSize = 10240
AuditLogRetentionPeriod = 0
RestrictGuestAccess = 1
[Application Log]
RestrictGuestAccess = 1
[Event Audit]
AuditSystemEvents = 3
AuditLogonEvents = 3
AuditObjectAccess = 3
AuditPrivilegeUse = 3
AuditPolicyChange = 3
AuditAccountManage = 3
AuditProcessTracking = 0
AuditDSAccess = 3
AuditAccountLogon = 3
[Registry Values]
MACHINE\Software\Microsoft\windows NT\CurrentVersion\winlogon\ScRemoveOption=1,"2"
MACHINE\Software\Microsoft\windows NT\CurrentVersion\winlogon\PasswordExpiryWarning=4,14
MACHINE\Software\Microsoft\windows NT\CurrentVersion\winlogon\ForceUnlockLogon=4,1
MACHINE\Software\Microsoft\windows NT\CurrentVersion\winlogon\CachedLogonsCount=1,"0"
MACHINE\Software\Microsoft\windows NT\CurrentVersion\winlogon\AllocateFloppies=1,"1"
MACHINE\Software\Microsoft\windows NT\CurrentVersion\winlogon\AllocateDASD=1,"0"
MACHINE\Software\Microsoft\windows NT\CurrentVersion\winlogon\AllocateCDRoms=1,"1"
MACHINE\Software\Microsoft\windows NT\CurrentVersion\Setup\RecoveryConsole\SetCommand=4,0
MACHINE\Software\Microsoft\windows NT\CurrentVersion\Setup\RecoveryConsole\SecurityLevel=4,0
MACHINE\Software\Microsoft\windows\CurrentVersion\Policies\System\UndockwithoutLogon=4,0
MACHINE\Software\Microsoft\windows\CurrentVersion\Policies\System\ShutdownwithoutLogon=4,0
MACHINE\Software\Microsoft\windows\CurrentVersion\Policies\System\LegalNoticeText=7,
MACHINE\Software\Microsoft\windows\CurrentVersion\Policies\System\LegalNoticeCaption=1,""
MACHINE\Software\Microsoft\windows\CurrentVersion\Policies\System\DontDisplayLastUserName=4,1
MACHINE\Software\Microsoft\windows\CurrentVersion\Policies\System\DisableCAD=4,0
MACHINE\Software\Microsoft\Driver Signing\Policy=3,2
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireStrongKey=4,1
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireSignOrSeal=4,1
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SealSecureChannel=4,1
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SignSecureChannel=4,1
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RefusePasswordChange=4,0
```

**Figure 2- Security Template Example/Text Version**

```
hisecdc - Notepad
File  Edit  Format  View  Help
MACHINE\Software\Microsoft\windows NT\CurrentVersion\winlogon\PasswordExpirywarning=4,14
MACHINE\Software\Microsoft\windows NT\CurrentVersion\winlogon\ForceUnlockLogon=4,1
MACHINE\Software\Microsoft\windows NT\CurrentVersion\winlogon\CachedLogonsCount=1,"0"
MACHINE\Software\Microsoft\windows NT\CurrentVersion\winlogon\AllocateFloppies=1,"1"
MACHINE\Software\Microsoft\windows NT\CurrentVersion\winlogon\AllocateDASD=1,"0"
MACHINE\Software\Microsoft\windows NT\CurrentVersion\winlogon\AllocateCDRoms=1,"1"
MACHINE\Software\Microsoft\windows NT\CurrentVersion\Setup\RecoveryConsole\SetCommand=4,0
MACHINE\Software\Microsoft\windows NT\CurrentVersion\Setup\RecoveryConsole\SecurityLevel=4,0
MACHINE\Software\Microsoft\windows\CurrentVersion\Policies\System\UndockWithoutLogon=4,0
MACHINE\Software\Microsoft\windows\CurrentVersion\Policies\System\ShutdownWithoutLogon=4,0
MACHINE\Software\Microsoft\windows\CurrentVersion\Policies\System\LegalNoticeText=7,
MACHINE\Software\Microsoft\windows\CurrentVersion\Policies\System\LegalNoticeCaption=1,""
MACHINE\Software\Microsoft\windows\CurrentVersion\Policies\System\DontDisplayLastUserName=4,1
MACHINE\Software\Microsoft\windows\CurrentVersion\Policies\System\DisableCAD=4,0
MACHINE\Software\Microsoft\Driver Signing\Policy=3,2
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireStrongKey=4,1
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireSignOrSeal=4,1
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SealSecureChannel=4,1
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SignSecureChannel=4,1
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RefusePasswordChange=4,0
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\MaximumPasswordAge=4,30
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\DisablePasswordChange=4,0
MACHINE\System\CurrentControlSet\Services\NTDS\Parameters\LDAPServerIntegrity=4,2
MACHINE\System\CurrentControlSet\Services\LDAP\LDAPClientIntegrity=4,1
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnablePlainTextPassword=4,0
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\RequireSecuritySignature=4,0
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnableSecuritySignature=4,1
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\AutoDisconnect=4,15
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableForcedLogOff=4,1
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\RequireSecuritySignature=4,1
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableSecuritySignature=4,1
MACHINE\System\CurrentControlSet\Control\Session Manager\ProtectionMode=4,1
MACHINE\System\CurrentControlSet\Control\Session Manager\Memory Management\ClearPageFileAtShutdown=4,1
MACHINE\System\CurrentControlSet\Control\Session Manager\Kernel\ObCaseInsensitive=4,1
MACHINE\System\CurrentControlSet\Control\Print\Providers\LanMan Print Services\Servers\AddPrinterDrivers=4,1
MACHINE\System\CurrentControlSet\Control\Lsa\SubmitControl=4,0
MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymousSAM=4,1
MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymous=4,1
MACHINE\System\CurrentControlSet\Control\Lsa\NoLMHash=4,1
MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\NTLMMinServerSec=4,0
MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\NTLMMinClientSec=4,0
MACHINE\System\CurrentControlSet\Control\Lsa\LmCompatibilityLevel=4,5
MACHINE\System\CurrentControlSet\Control\Lsa\FullPrivilegeAuditing=3,0
MACHINE\System\CurrentControlSet\Control\Lsa\EveryoneIncludesAnonymous=4,0
MACHINE\System\CurrentControlSet\Control\Lsa\DisableDomainCreds=4,1
MACHINE\System\CurrentControlSet\Control\Lsa\CrashOnAuditFail=4,0
MACHINE\System\CurrentControlSet\Control\Lsa\AuditBaseObjects=4,0
[Version]
signature="$CHICAGO$"
Revision=1
[Profile Description]
Description=A superset of securedc. Provides further restrictions on LanManager authentication and further requirements for
the encryption and signing of secure channel and SMB data.  In order to apply hisecdc to a DC, all of the DC's in all trusted
or trusting domains must be running Windows 2000 or later. See online help for further info.
```

**Figure 3- Security Template Example/Text Version**

As you can see, although the policy is a simple text .INF file, the Security Template Tool within the MMC, is much more intuitive to edit and manage. The Security Template is made up of a default set of categories, or groupings. Within these categories, there are several policies that can be set to apply the desired security settings.

## 2.0 System Description

The Deployment of a system security configuration template needs to take many factors into account. Perhaps the most important factor, is the role that the system will perform. Will the system in question be a critical part of your network infrastructure?  Have you done an Asset identification and classification as part of your network security policy? If you have, it is advised to review this document prior to the design and implementation your Security Template. How will the system be accessed? By Whom?  What services will this server require in order to perform it's required functions? What applications, if any will be installed on this system? How will this system communicate with other systems on your network? Who will have access to the machine? Both logical access through the network, as well as physical access to the server?  Several of the settings that we will be testing and discussing deal with locally logged on users. In this case, it is important to understand who

will have physical access to the system, what it is they will need to do, and what they should not be able to do while logged on locally. The answers to these questions and a solid understanding of each setting within a Security Template are required in order to implement a configuration that will serve as one pillar in the foundation of your security posture.

### 2.1 System Role

As I said earlier, the system in question will be acting as a Web Content filtering server. The server will also be running Windows Terminal Services in remote administration mode. The physical location of the system is a rack in my home office. Physical as well as logical access to the machine will be limited to only me. No access to the system will be available from the Internet. The Test server is Dual-Homed, and all machines in my home/test network are configured to use the "internal interface" of the Test server as their default gateway. The external interface is connected to a Linksys DSL router. The router is then connected to my DSL modem for external internet access. The System, once testing is completed, will go live into fictional company XYZ. Company XYZ is a service company that provides outsourced healthcare program management services to enterprises around the world. The organization has 120 Windows 2000 Servers running various applications and software. 14 of these servers are domain controllers, with 4 of them located at the central office/data center. The remaining 10 are physically located at the remote office locations. Company XYZ is a single domain environment that is fully Active Directory enabled.

### 2.2 System Software

The system used in my test environment is running Windows 2000 server with Service Pack 3. In addition to the System Software, the test server was running SuperScout Web Filter V4.1 from SurfControl, Microsoft Office XP, McAfee VirusScan Home Edition 7.0, ZoneAlarm Pro v3.5, as well as Microsoft Baseline Security Analyzer (MBSA) V 1.1.

### 2.3 Additional "Hardening" procedures

When designing a secure system, you should start with the basic architecture of the system. The answers to the questions Mentioned above in section 2.0, 'System Description', will help determine what software as well as services will be installed and/or running on the machine. It is best to have the answers to the questions before you start. When installing a system with security as one of the goals, you should start with a clean install. After the initial installation, the system needs to reboot, and start back up. At this point, I began to remove services that were not needed, but unable to render inoperative during the installation. Because of many service dependencies and functions, it is easier to define what should be left on for the requisite functionality, and disable everything not needed.

Below is a list of the services that were running on the test computer.

SERVICES:

| | |
|---|---|
| DNS Client | RunAs service |
| EventLog | Security Accounts Manager |
| IPSec Policy Agent | Net Logon |
| Logical Disk Manager | Terminal Services |
| Network Connections Manager | Terminal Services Licensing |
| Plug & Play | File Replication Service |
| Protected Storage | Windows Time |
| Remote Procedure Call | Kerberos Key Distribution Center |
| Remote Registry Service | RPC Locator |
| Server | Workstation |
| SuperScout Report Service | SuperScout Scheduler Service |
| SuperScout Web Filter Service | System Event Notification |

Each of the services listed above were set to start automatically. Through trial and error, along with additional research [1], it was determined that these services were/are the absolute minimum required to operate a secure server, as my Content filtering server.

## 2.4 System Hardware

The test server I used was a Compaq DL 320, running Windows 2000 Server. Processor is a Pentium III 933 MHz. There is 1 Gigabyte of RAM  installed on the machine. The hard disks are 2 / 40 gig drives in a mirrored configuration.  The system has a CD-Rom and 3.5" floppy drive. For network access the system has 2 Compaq NC 3163 Fast Ethernet NIC's onboard.

**3.0 Security Template Selection**

For the Template selection, I have chosen to use Win2k_Server.INF, created by the National Security Agency (NSA). Although Microsoft provides several baseline templates used to help secure the OS, I chose to use a template supplied/created by an independent organization. The security requirements of the system in question dictate that only I have access to this system, both physically as well as logically. This system once fully tested, will be put into operations inside organization XYZ, as the active Web Content Monitor. One of the major requirements of this system, is maintaining the integrity of data collected. In some cases, the data collected will be used for disciplinary action, or performance reviews. Given this set of security requirements, I opted to select what I felt would be the more restrictive, hence secure, template that I could. Given the reputation the NSA has for security, I felt I made the proper selection. It is expected that once the template is applied, further configurations and "tweaking" will need to be done in order to have a secure system that is functional as a Content monitor. The expectation from the Vice President of organization XYZ. Is that, once the system is operational, she will be able to go to her Directors and inform them that she has a system in place to monitor all employees internet access. The Vice President wants/needs to be able to tell her Directors that the system in place to monitor users, is secure, is "outside" of the IT organization, and access is only available to ONE person, her Sr. Security Engineer.

*3.1 Security Template Settings*

The template created by the National Security Agency is freely available from their web site, http://nsa1.www.conxion.com/ [3] . The templates, along with the Microsoft Security and Configuration tool set, allow for the deployment of a common set of security configurations to multiple computers or users within an organization. As mentioned before, a Security Template is a physical representation of a number of common, and some not so common security configurations. Below is a list of the major configurations that can be changed within a Security Template. I will explain the ones used in my evaluation in more detail as we move through the test.

- o Account Policies – Includes Password Policy, Kerberos Policy, Account Lockout Policy
- o Local Policies – Includes Audit Policy, User Rights Assignment, and numerous Security Options
- o Event Log – Includes settings for the Event Log
- o Restricted Groups – Includes membership settings for sensitive groups
- o System Services – Defines configuration settings for System Services
- o Registry – Allows you to set stricter DACL's (Discretionary Access Control List) for various registry keys
- o File System -- Allows you to set stricter DACL's (Discretionary Access Control List) for various system folders and files.

### 3.2 Relevant changes

### 3.3 Account Policies

Account Policy settings are where Password relevant security configuration settings are made. Within account policies, the relevant settings that were tested/set are:

*Enforce Password History – 24 Passwords remembered.*
With this setting we are preventing the users from using their favorite passwords over and over again. A user must cycle through 24 different passwords before they are able to re-use a specific word or pass-phrase. With a *Minimum Password Age* of 1 day, (Which I will discuss in a moment), a specific password cannot be used again for at least 24 days. This reduces the opportunity for the password to be guessed by unauthorized users.

*Maximum Password Age – 90 Days*
The Maximum Password Age is the "Lifetime" that a password is considered valid for a specific user. In many environment 90 days is sufficient, while in situations that require a higher level of security 90 days could be considered too long of a "Lifetime". Given the fact that the *Minimum Password Length* (Discussed in a moment) is 12 Characters, I felt that a Password "Lifetime" of 90 days was sufficient.

*Minimum Password Age – 1 Day*
This setting dictates how long a user must keep a specific password, before changing it again. When used in conjunction with the *Enforce Password History* we are able to create an environment where users are not continuously re-using the same passwords. One could think of this as a small hurdle in our "Defense in Depth" strategy.

*Minimum Password Length – 12 Characters*
Password strength is largely determined by its length. If a password is too short (a relative term I know) then it can be easily guessed or cracked. There are numerous free tools available on the internet that can quickly crack inadequate passwords. This password option requires that a password have a minimum of 12 characters. When used with the next option (*Passwords must meet complexity requirements)* the chances of passwords being cracked with one of the above mentioned free tools is greatly reduced. Without going into great detail surrounding password encryption and cryptography, I will say that Password Length is more important than Password Complexity when it comes to creating a strong password.

*Passwords must meet complexity requirements – Enabled*
Complex passwords provide a certain measure of defense against password cracking. This option forces the use of a Dynamic Link Library (DLL) called *passfilt.dll* by all users. This DLL requires that passwords meet a certain level of complexity, as dictated by the DLL. Specifically, passwords must contain characters from 3 of 4 special classes; Lower Case letters, Upper Case letters, Numerals, and Special Characters. In addition to these requirements, the DLL ensures that passwords cannot be the same as the User's Login ID.

Given the security requirements set forth by the Vice President, I felt that a strong password policy was essential to meet those requirements. If this option is enabled, with user accounts and passwords already created on the system, the complexity requirements will NOT take effect until the user changes his/her password. Passwords that already exist are not subjected to the *passfilt.dll* complexity requirements.

*Store Passwords using reversible encryption for all users in the domain – Disabled*
This option will determine whether or not you want to store passwords with a "2-way Hash" function. There are very few reasons for ever enabling this option, as it reduces the security of stored passwords. As such, it remains disabled for this test.

### 3.3.1 Account Lockout Policy

*Account Lockout Duration – 15 minutes*

This option defines how long an account will be "Locked Out" from further logon attempts after the *Account Lockout Threshold* has been violated. The options here are anywhere from 0 (Account is locked out until an administrator unlocks it. This used to be a selection in NT 4.0 Account Policy) to 99999 minutes.

*Account Lockout Threshold – 3 invalid logon attempts*

With this setting we are attempting to prevent endless password guessing through a "brute-force" or "dictionary" attack.  This options dictates that when a particular user ID has supplied the wrong login credential (Password) for a specified number of attempts (3 in our case), the account is "locked out" from further access attempts.

*Reset Account Lockout after – 15 minutes*

Sets the time length, in minutes, until the invalid logon count is reset. In my test server with the NSA template, it was set to 15 minutes. So, if the *Account Lockout Threshold* is set to 3, and there are 2 invalid logon attempts, waiting 15 minutes will reset the counter back to zero.

### 3.3.2 Kerberos Policy

As Kerberos is the default authentication scheme in a Windows 2000 Active Directory environment, Active Directory is necessary for Kerberos authentication. The Kerberos policy settings only apply at the domain level, thus they should be defined in the Domain Group Policy Object. They were not used, or altered in my practical.

### 3.4 Local Policies

Within the Local Policies option of a Security Template, there are several categories of configurable items.

3.4.1 Audit Policy

*Audit account logon events – Success, Failure*

This policy setting determines whether or not you will audit each instance of a user logging on to, or off from another computer, when this local computer is used to validate the account credentials. The Security Template I will be using has the settings configured to audit both successful, as well as failed account logons.

*Audit account management – Success, Failure*

This template settings determines whether or not to audit each event of account management on a system. Some of the various events that would dictate use of account management are:

- Creation of a User account or Group
- A User account is renamed, disabled, or enabled.
- Anytime a password is set or changed.

*Audit directory service access – Not defined*

This setting determines whether or not to audit an individual user accessing an Active Directory object that has its own System Access Control list. This setting is not defined in this template.

*Audit logon events – Success, Failure*

Tracks each instance of a user logging on, logging off, or establishing a network connection. This option records where the logon occurred, versus where the logged-on account resides. "Account Logon Events" are generated where the account resides, "Logon Events" are generated where the logon occurs.

*Audit object access – Failure*

Tracks unsuccessful attempts to access directories, files, printers or other "objects". In order for this to be successful, auditing must be enabled on the individual objects properties.

*Audit policy change – Success, Failure*

This setting tracks every incident of a change to user rights assignment policies, changes in the audit policy, security policy, and trust policies.

*Audit privilege use – Failure*

This setting will generate an audit entry when the exercise of a User Right fails. This entry tracks all user rights with the exception of the following:

- Bypass Traverse Checking
- Debug programs
- Creation of a Token Object
- Replace Process Level Token
- Generate Security Audits
- Backup files and directories
- Restore files and directories

*Audit process tracking – No auditing*

Tracks program activation and exits. This setting is set to No auditing.

*Audit system events – Success, Failure*

This setting determines whether to audit the rebooting or shutting down of a system. Also any event that affects the system security or security log is audited.

3.4.2 User Rights Assignment

Within the User Rights Assignment option under Local Policies, there are 34 different security configuration options. In this paper, I will only be discussing those that are defined in the NSA Security Template.

*Access this computer from the network – Administrators*

This setting allows a user to connect to the system over the network. On this setting, I varied from the NSA template. As this system will be a monitoring server, I did not want users to access the machine. As such, I restricted access to only the Administrators.

*Back up files and directories – Administrators*

This setting determines which users can circumvent file and folder permissions in order to backup the system. Only the administrators are given this right in the NSA template.

*Bypass Traverse Checking – Administrators*

This setting allows a user to change directories in order to access files and/or subdirectories even if the user has no permissions to access the parent directory. This right, does not allow the user to view/list the contents of the directories, Only to traverse them. Again, here I modified the NSA template and limited this right to only members of the Administrators group. I felt this was reasonable as legitimate access to this system will be limited to only 1 or 2 people.

*Change the system time – Administrators*

Defines which user and or group is allowed to change the system time/date on the internal clock of this computer.

*Create a pagefile – Administrators*

Determines who is authorized to change the size of, or create a "pagefile" for virtual memory use.

*Force shutdown from a remote system – Administrators*

Allows only the administrator to shut down the computer from a remote location over the network.

*Increase Quotas – Administrators*

Determines which user can use a process to access another process in order to increase the processor quota assigned to the other process.

*Increase Scheduling Priority – Administrators*

Determines which accounts are able to boost the execution priority of a process.

*Load and Unload Device Drivers – Administrators*

Allows only the administrators to install or remove device drivers.

*Log on Locally – Administrators*

Allows only the administrators to log on locally at this machine.

*Manage auditing and security log – Administrators*

Determines which user, or groups can specify object access auditing options for resource objects and registry keys.

*Modify firmware environment values – Administrators*

This setting allows only the Administrator to modify the system variables stored in nonvolatile RAM on the system.

*Profile Single Process – Administrators*

Determines which users are able to use Windows 2000 Performance Monitoring tools in order to monitor the performance of non-system processes.

*Profile System Performance – Administrators*

This setting determines which users are able to use Windows 2000 Performance Monitoring tools in order to monitor the performance of System Processes.

*Restore Files and Directories – Administrators*

Determines which users are able to circumvent file and folder permissions in order to restore backed up files and folders. Also determines which users can set any valid security principal as the owner of an object.

*Shut down the System – Administrators*

Determines which users that are logged on locally are able to shut down the system.

*Take ownership of files or other objects – Administrators*

Determines which users can take ownership of any object, such as a file or folder. One thing to note here is that with this right a user (Administrator) can take ownership of an object, however they cannot give ownership back.

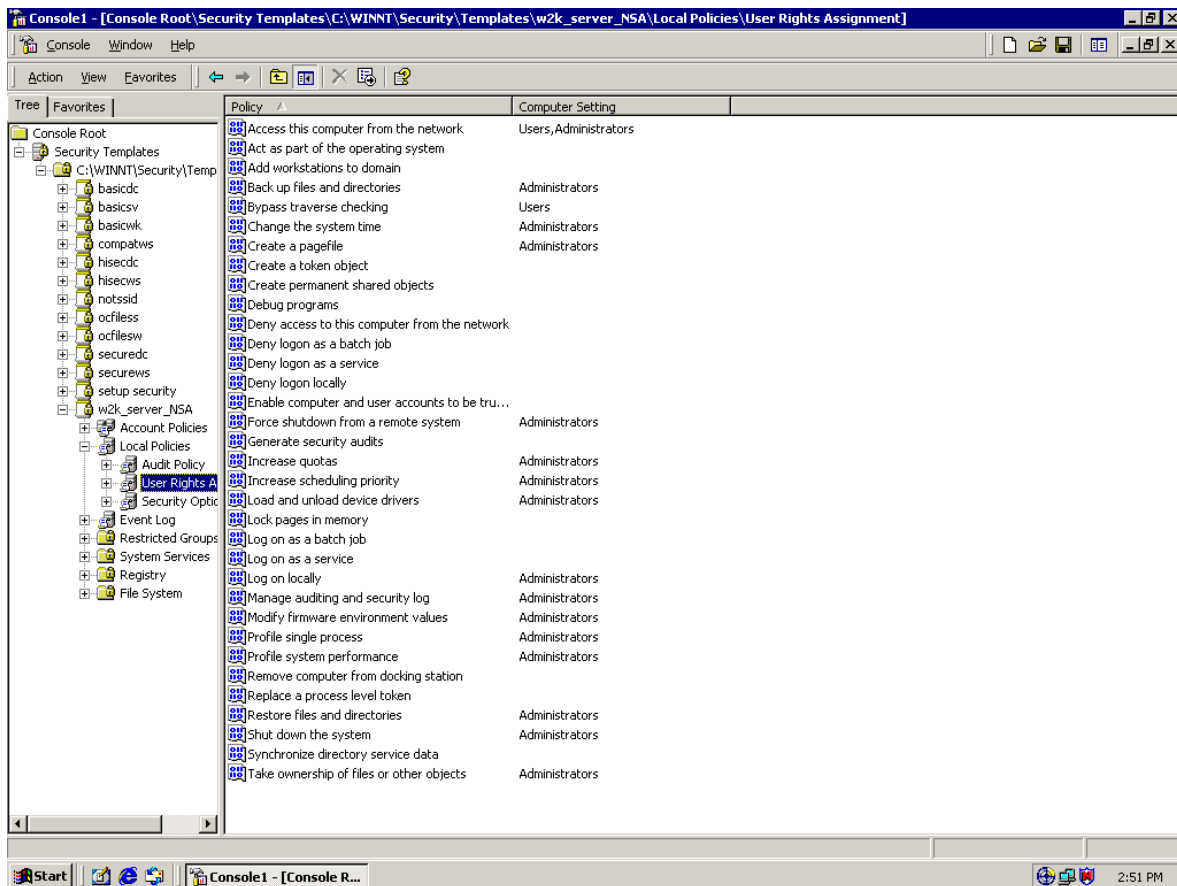Below is a screenshot of the MMC showing the *User Rights Assignment* configurations just discussed.

**Figure 4- MMC/User Rights Assignment options**

### 3.4.3 Security Options

Under the Security Options portion of our Security Template, we have 40 options that we can configure. These settings could be Enabled, Disabled, or simply Not Defined in the Template. Rather than discuss each of the Security Options, I will discuss the ones that are defined, and what the settings are for that option.

> *Additional restrictions for anonymous connections – No access without explicit anonymous permissions*

Here we are placing restrictions on anonymous users. The option selected requires that anonymous be given explicit permission to access network resources. The equivalent Registry setting for this option is:

HKLM\System\CurrentControlSet\Control\LSA\RestrictAnonymous = 2.

Please refer to Microsoft KB article Q246261 for more information on the possible ramifications of this setting. [4]

### *Allow system to be shut down without having to log on – Disabled*

With this policy disabled, the option to shut down the computer does not appear on the Windows logon screen. This forces the user to logon successfully and have rights to shut down the system.

### *Allowed to eject removable NTFS media – Administrators*

By default, Only members of the Administrators group are allowed to eject removable NTFS media. This setting also allows for the right to be given to *Power Users,* and *Interactive Users.*

### *Amount of idle time required before disconnecting session – 30 Minutes*

This setting determines the amount of idle time that must pass in an SMB (Server Message Block) session, before the session is terminated due to inactivity.

### *Audit use of Backup and Restore privilege – Enabled*

Determines whether or not you will audit every use of user rights including Backing up and Restoring. With this policy enabled, along with *Audit Privilege use,* then any instance of user rights being exercised will be recorded.

### *Automatically log off users when logon time expires (local) – Enabled*

This setting determines whether you will forcibly disconnect users that are connected to the local machine once their valid logon hours have passed.

### *Clear virtual memory pagefile when system shuts down – Enabled*

This setting wipes the system pagefile clean when the system shuts down, this ensures that confidential information that may be in the pagefile, is not available to unauthorized users.

### *Digitally sign client communication (when possible) – Enabled*

This setting enables an SMB client to perform digital packet signing when communicating with an SMB server. Digital signatures of SMB packet exchanges help to prevent "man in the middle attacks" of active SMB sessions.

*Digitally sign server communication (when possible) – Enabled*

This setting enables an SMB server to perform digital packet signing when communicating with an SMB server. Digital signatures of SMB packet exchanges help to prevent "man in the middle attacks" of active SMB sessions

*Disable CTRL+ALT+DEL requirement for logon – Disabled*

This setting determines whether the secure key sequence of CTRL + ALT + DEL is required in order to log into a system. If this policy is Enabled on a system, then a user is NOT required to press CTRL + ALT + DEL in order to logon. The CTRL + ALT + DEL sequence ensures a "trusted path" to the operating system, and should not be circumvented.

*Do not display last user name in logon screen – Enabled*

Determines whether the name of the last logged on user is displayed in the Windows logon screen at next login. With this policy Enabled, the username of the last successful logon is Not displayed in the winlogon dialog box.

*LAN Manager Authentication Level – Send NTLM v2 response only\refuse LM & NTLM*

This setting specifies the method of Challenge/Response authentication to be used for network logons with down-level clients. LM and NTLM are relatively insecure authentication methods, however NTLMv2 is a more robust/secure version of Challenge/Response. This option requires that only NTLM v2 responses will be accepted. This option corresponds to a registry value of 5

HKLM\System\CurrentControlSet\Control\LSA\LMCompatibilityLevel = 5

A great article for further understanding of these options is Microsoft's KB article Q272129 [5]

*Message text for users attempting to log on – "Secure System! Authorized Users Only, Unauthorized use of this system will be monitored and users will be punished accordingly."*

This message is used to warn unauthorized users as to the secure nature of the system. There have been several rumors in the IT industry of users escaping prosecution for unauthorized access because the Lack of a warning banner was construed as an invitation.

*Message title for users attempting to log on – Authorized Users Only*

Used in conjunction with the Message text box, this is the Title of the warning dialog box.

*Number of previous logons to cache (in case domain controller is unavailable) – 0 logons*

Windows 2000, by default, caches the previous 10 successful logons for system availability. This feature is useful for mobile users (laptops) who need to access their systems during times when they are not connected to the domain or when domain controllers are unavailable. The template supplied by the NSA changes this to 0 logons being cached.

*Prevent system maintenance of computer account password – Disabled*

By default, Computer systems change their account passwords every seven days. Enabling this option prevents the machines from requesting a new password weekly. Setting this option to Disabled will allow a new password to be generated every seven days.

*Prevent users from installing printer drivers – Enabled*

This setting prevents users from installing print drivers that have not been previously installed on the local machine. With this option Enabled, users are still able to connect to Network Printer to which they have the user rights to.

*Prompt user to change Password before expiration – 14 days*

Here we are determining how far in advance we will warn users that their passwords will expire. The NSA template has this set at *14 days.* Thus, the user will receive a warning *14 days* prior to their password expiring, that their password will expire, and giving them the option of changing it at that time.

*Recovery Console: Allow automatic administrative logon – Disabled*

By default, when accessing the system through the Recovery Console, administrators are required to provide a password to access the Console, Enabling this setting does not require a password, and will automatically log a user on to the system.

*Recovery Console: Allow floppy copy and access to all drives and folders –Disabled*

This setting enables or disables the Recovery Console SET command, which allows the setting of various environment variables within the Console.

*Rename administrator account – Enabled*

This option allows you to associate a different username with the Security Identifier (SID) that is normally assigned to the administrator. Changing the administrators username is a small hurdle you can place in front of would be intruders. Here is another setting that I

personally altered from the NSA template. The NSA template had this setting configured locally, while I opted to Enable it, and change the administrator username.

### Rename guest account – Enabled

This option allows you to associate a different username with the Security Identifier (SID) that is normally assigned to the built in guest account. Changing the guest username is a small hurdle you can place in front of would be intruders. Here is another setting that I personally altered from the NSA template. The NSA template had this setting configured locally while I opted to Enable it, and change the guest username in addition to the administrators.

### Restrict CD-ROM access to locally logged-on user only – Enabled

This setting, when enabled, dictates whether a CD-ROM is available to users both local, and across the network concurrently. If *Enabled* only the user logged in interactively is allowed to access the CD-ROM. However, if no one is logged on interactively, the CD-ROM is available to be shared over the network

### Restrict floppy access to locally logged-on user only – Enabled

This setting, when enabled, dictates whether a Floppy Drive is available to users both local, and across the network concurrently. If *Enabled* only the user logged in interactively is allowed to access the Floppy Drive. However, if no one is logged on interactively, the Floppy Drive is available to be shared over the network.

### Secure channel: Digitally encrypt secure channel data (when possible) – Enabled

This security option setting determines whether a domain member computer will attempt to negotiate an encryption scheme/key for all secure traffic that it initiates. Once a computer is joined to the domain, it has a computer password, every time that system restarts, it uses that password to establish a secure channel with a domain controller. With this setting enabled, the domain member will attempt to negotiate encryption for that secure channel.

### Secure channel: Digitally sign secure channel data (when possible) – Enabled

With this setting we are determining whether a domain member attempts to negotiate digital signing for all secure channel traffic that it initiates

### Shut down system immediately if unable to log security audits – Enabled

When enabled, as it is in the template I am using, the system will shut down if it is unable to log security events to the Windows Event Viewer logs. With this option

enabled, and the Security log full, any new alerts will be unable to be written to the security log. When this happens the following Stop error appears:

**STOP: C0000244 {Audit Failed}**
**An attempt to generate a security audit failed.[6]**

To recover from this Stop Error, an administrator must log on, clear the log, and reset this option. Until this security setting is reset, only a member of the Administrators group will be able to log on to the system, even if the security log is not full.

### *Smart Card removal behavior – Lock Workstation*

If users are logged on using Smart Cards, what happens when the Smart Cards are removed from the system? This setting determines that action. When *Lock Workstation* is set, the workstation is locked when the Smart Card is removed, allowing the user to leave their system unattended, while still maintaining their secure session.

### *Strengthen default permissions of global system objects (e.g. Symbolic links) – Enabled*

Strengthens the Discretionary Access Control Lists (DACLs) of the global list of shared system resources, allowing a user with non-administrative permissions to read/view, but not modify objects they did not create.

### *Unsigned driver installation behavior – Warn but allow installation*

Sets the action that will occur when a device driver that has not been certified for Windows 2000 attempts to load. As I have set the machine up so that both physical as well as logical access to the machine is quite secure, I felt staying with the default setting created by the NSA was adequate.

### *Unsigned non-driver installation behavior – Warn but allow installation*

Sets the action that will occur when a non-device driver that has not been certified for Windows 2000 attempts to load. As I have set the machine up so that both physical as well as logical access to the machine is quite secure, I felt staying with the default setting created by the NSA was adequate.

**3.5 Event Log**

*Maximum security/application/system log size – 4194240 kilobytes*

With log file maximums set too low, the administrators must save, and clear the logs more often, in order to prevent system shutdown. ( See Security options above.) This setting allows the log file to fill to either the maximum available space on the drive, or 4GB (Whichever is smaller) before halting the system. The available ranges are from 64KB to 419240KB.

*Restrict guest access to application/security/ and system logs – Enabled*

In a default configuration, guests and "null logons" are given the ability to view event logs. (System and Application only) This option, when enabled, prohibits guests and "null logons" from viewing any of the event logs.

*Retention method for application/system/security logs – Manually*

Determines how the operating system will handle event logs once they have reached the maximum allowable size. *Manually* dictates that the logs will NOT be overwritten, and must be cleared manually. This ensures that no data will be lost as a result of logs being overwritten.

*Shut down the computer when the security audit log is full – Enabled*

When security events cannot be written to the Security Log, the system should be shut down immediately. If the system does shut down as a result of this setting, only a member of the administrators group is able to log on, and he/she must clear the log.

**3.6 Restricted Groups**

The Restricted Groups setting allows the Administrator to control the membership of sensitive groups.  With this policy setting, you can specify what members (users) are a member of a specific group. Any members not specified in the policy, are removed from the group during the next policy refresh.

*Restricted Groups – Power Users*

The *Power Users* group is automatically included in the *Restricted Groups* policy since it is a Windows 2000 default group. The NSA template provides this setup with the *Powers Users* having no members. As such, if any user account is placed in the *Powers Users* group, they will be removed at the next policy refresh. This policy option will help against both intentional, unintentional, and nefarious cases of privilege escalation.

**3.7 System Services**

The System Services configuration options within the Security template allow an administrator to define and lock down the start up mode, and the access permissions for all System Services. Due to the fact that System Services are very enterprise specific, they are not defined in this template. For this practical, I have chosen to leave them as such, and rely upon the manual "hardening" process that was discussed earlier.

**3.8 Registry values modified**

The Security and Configuration Tool Set can be used to configure (DACLs) Discretionary Access Control Lists for various registry keys. The Tools set provided with Windows 2000 allows for 31 various registry keys permissions to edit. Permissions on registry keys are similar to file DACLs in that they are able to inherit permissions from their "parent" object. Additional permissions can be defined for a child object in addition to those inherited from it's "parent".

The Template created by the NSA set configuration changes for the following registry Hives:

- ♦ HKEY_CLASSES_ROOT\
- ♦ HKEY_LOCAL_MACHINE\
- ♦ HKEY_USERS\

For this paper, I will not go into detail on each specific registry Hive, Key, or the settings on each. I felt that the NSA settings were adequate, with the exception of the "Users" group. In all Registry Key settings where the "Users" group was given a specific permission, I substituted the group "Authenticated Users".
Below is a screen shot of the Registry Hives and their settings with the NSA template applied.
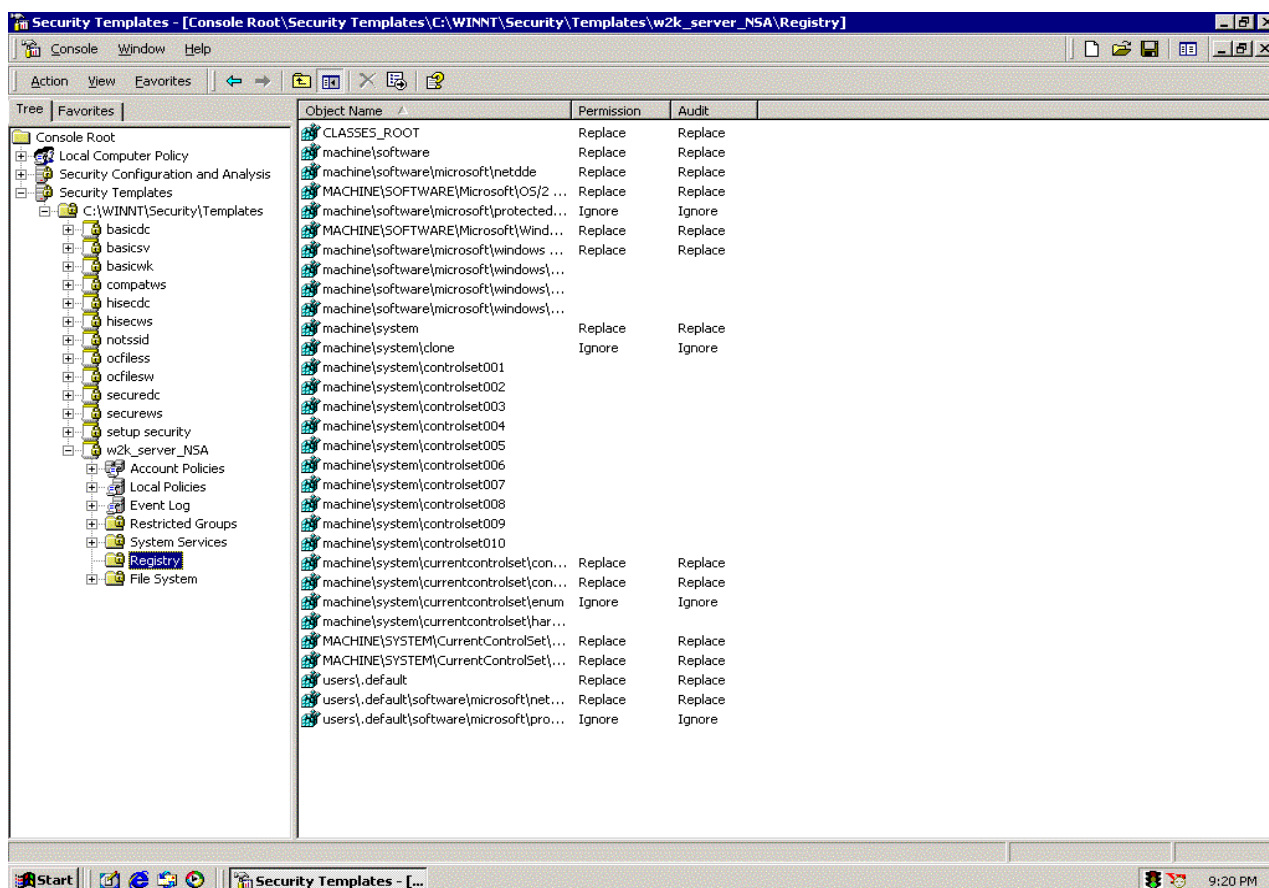
**Figure 5 –Registry Security Settings**

### 3.9 File System Security

The use of the NTFS file system should be a requirement of all new and existing systems. The benefits of using NTFS far outweigh most any reason that a person could think of for Not using it. With NTFS as a file system, you gain the ability to audit things like "file and object access", "use of user rights",  "policy change", "logon and logoff events", etc…

In addition to the ability to audit actions on the file system, you have the ability to set permissions to individual files, at a local level. Meaning that the permissions will apply, even if a user is able to access the file on the machine, or server the effective permissions defined for that user will be applied. This is unlike "share permissions" that actually only apply across a network.  File size on an NTFS volume is limited, in theory at least, only by the actual volume size. While FAT32 has a practical limit of 4GB's. NTFS supports File and Folder compression, NTFSv5 supports Encryption as well. Neither FAT16, nor FAT32 provides these features.

The File System Security options of the NSA Template provide for setting the security parameters on 58 crucial directories and subdirectories. Such as:

- ♦ **%System Root%**
- ♦ **%System Drive%**
- ♦ **%System Directory%**
- ♦ **%Program Files%**

As those are too many to list for this practical, and my decision to stay with the NSA defaults, I will not talk to each one. For more in depth reading on the File System Security settings in the NSA template see: http://www.nsa.gov/snac/win2k/index.html

**4.0 Applying the Template**

Ok, now we've gone through the majority of the Security Template configuration settings in detail. The next thing we have to do is, using the Security Configuration and Analysis Tool mentioned earlier, actually Apply the Template to my test server. The following will walk us through applying the template step by step. In order to apply the template, we must open the MMC and use the Security Configuration and Analysis tool.

1. Select start, 'Run', in the Run box, type "MMC". This will open the "empty shell" that is the MMC. The MMC itself provides nothing more than a common framework for the "Snap-ins" to use.
2. From the 'Console' menu option select 'Add/Remove Snap-in'.
3. Click 'Add' on the Add/Remove Snap-in dialog box.
4. Select the Security and Configuration Analysis Snap-in.
5. Select 'Add' → Close → OK
6. Under the Console Root in the MMC select Security Configuration and Analysis.
7. Right click, and select either open database, here you can create a new database, or open an existing database. I opted to create a new database called "NSA_Secure.sdb"
8. Click Open
9. When prompted to open the '.inf' file, select the '.inf' file associated with your template. My file was named, "NSA.inf.
10. Click Open

Now, We apply the template.
1. Once again, right click on Security Configuration and Analysis.
2. Select "Configure Computer Now"
3. In the "Configure System" dialog box, you will be prompted to supply a name and location for the error log file.
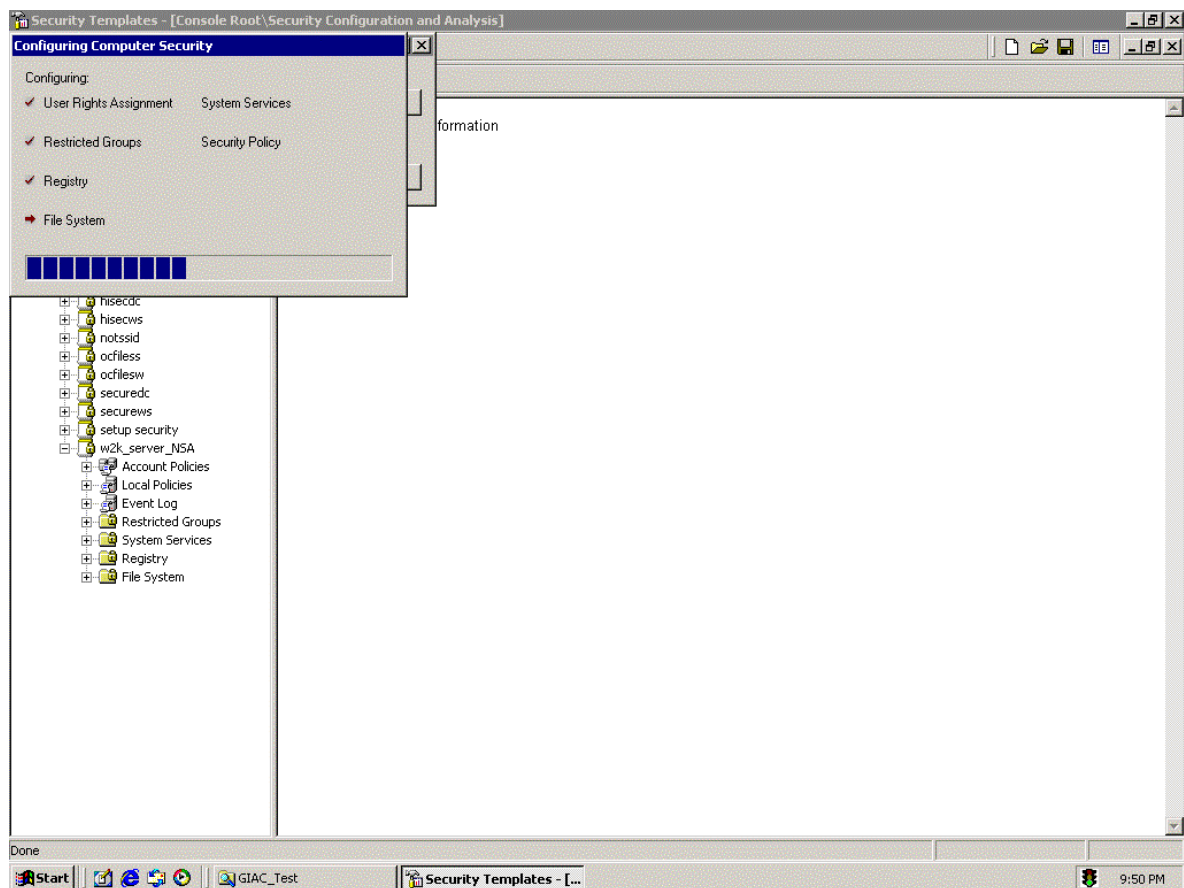4. Click OK

See Figure 6 Applying the Template

**Figure 6 – Applying the Template**

Once the Template is applied, a good recommendation is to use the Analysis portion of the Security Configuration and Analysis tool to verify the settings are being applied as you planned.

1. Right Click on the Security Configuration and Analysis tool once again.
2. This time, select ' Analyze Computer now'. See the Figure 7
3. In the 'Perform Analysis' dialog box, enter a name and path for the error log.
4. Select OK.  See figure 9 for analysis progress.
5. When analysis is done, the settings applied will have a green check mark next to them. Any settings not applied will have a red X next to them.
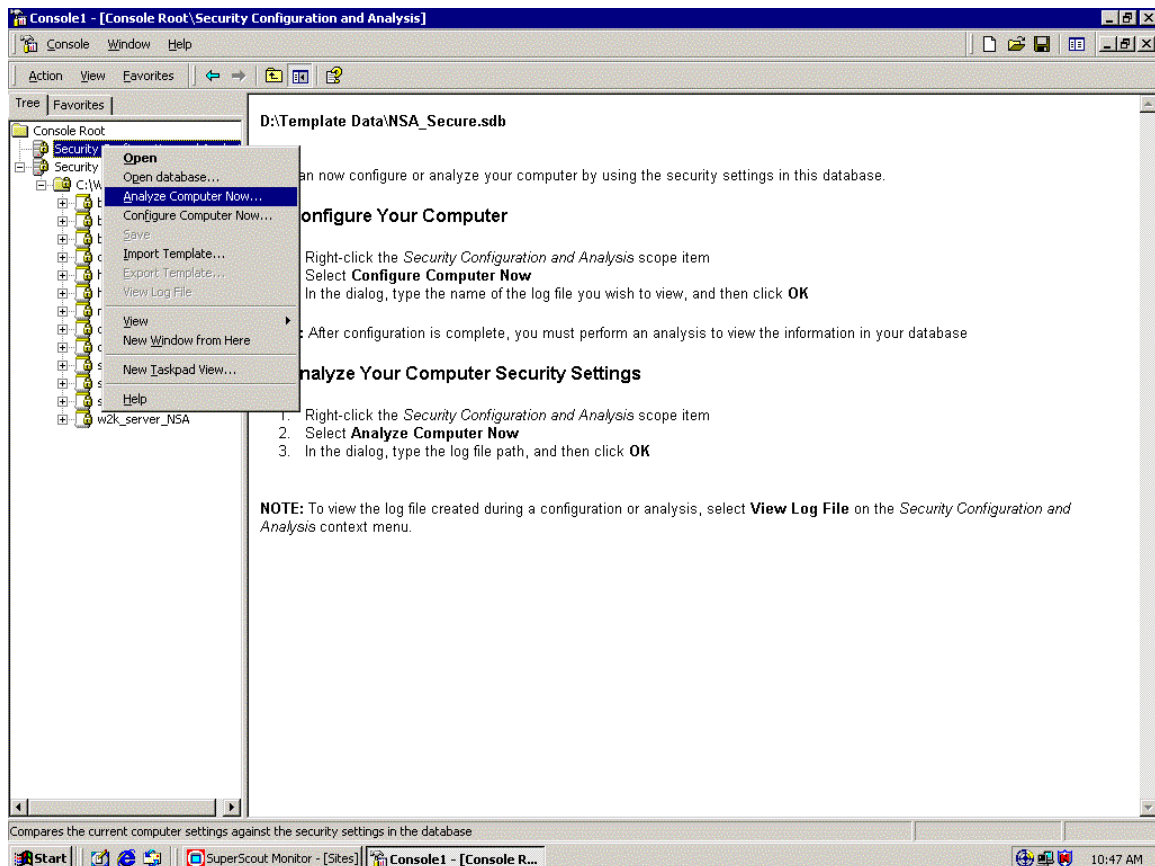
**Figure 7 – Analyzing Computer Security Settings**
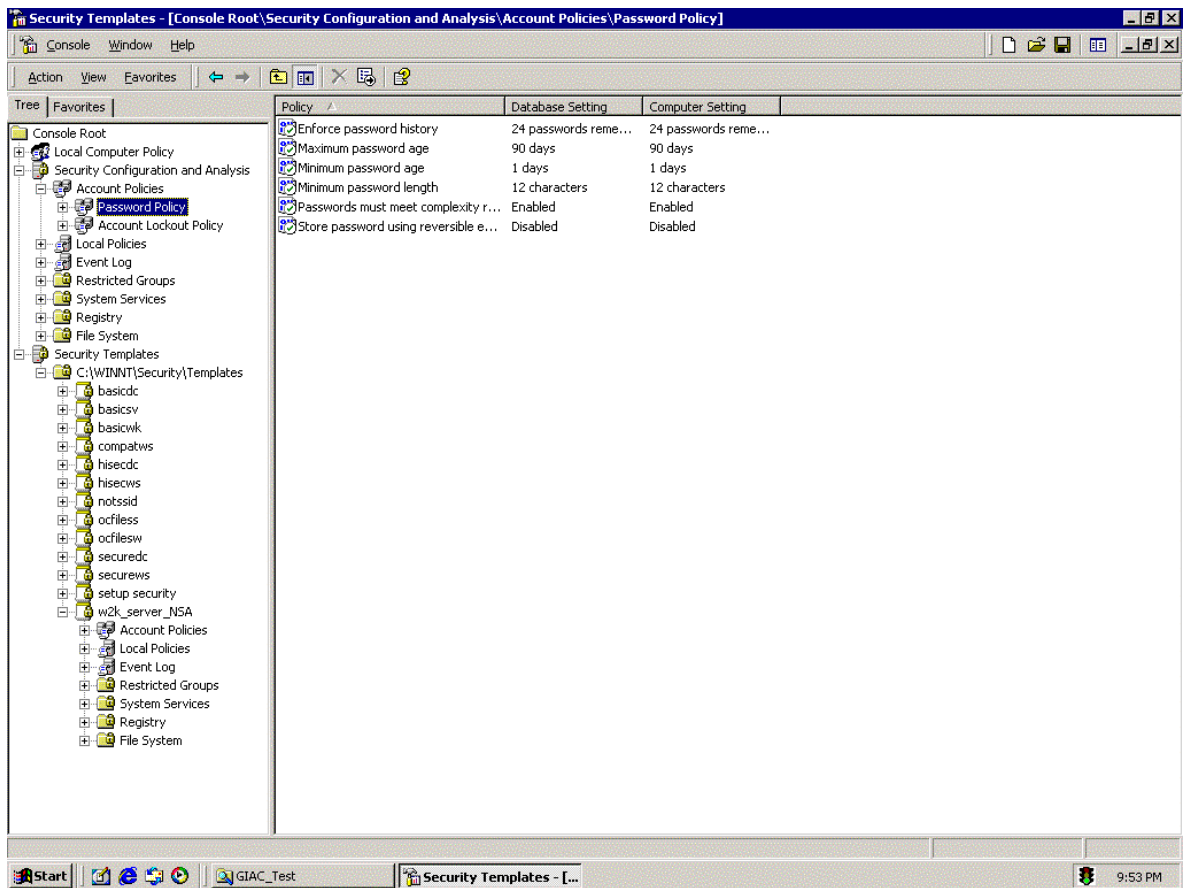
**Figure 8 – Analyzed Settings**
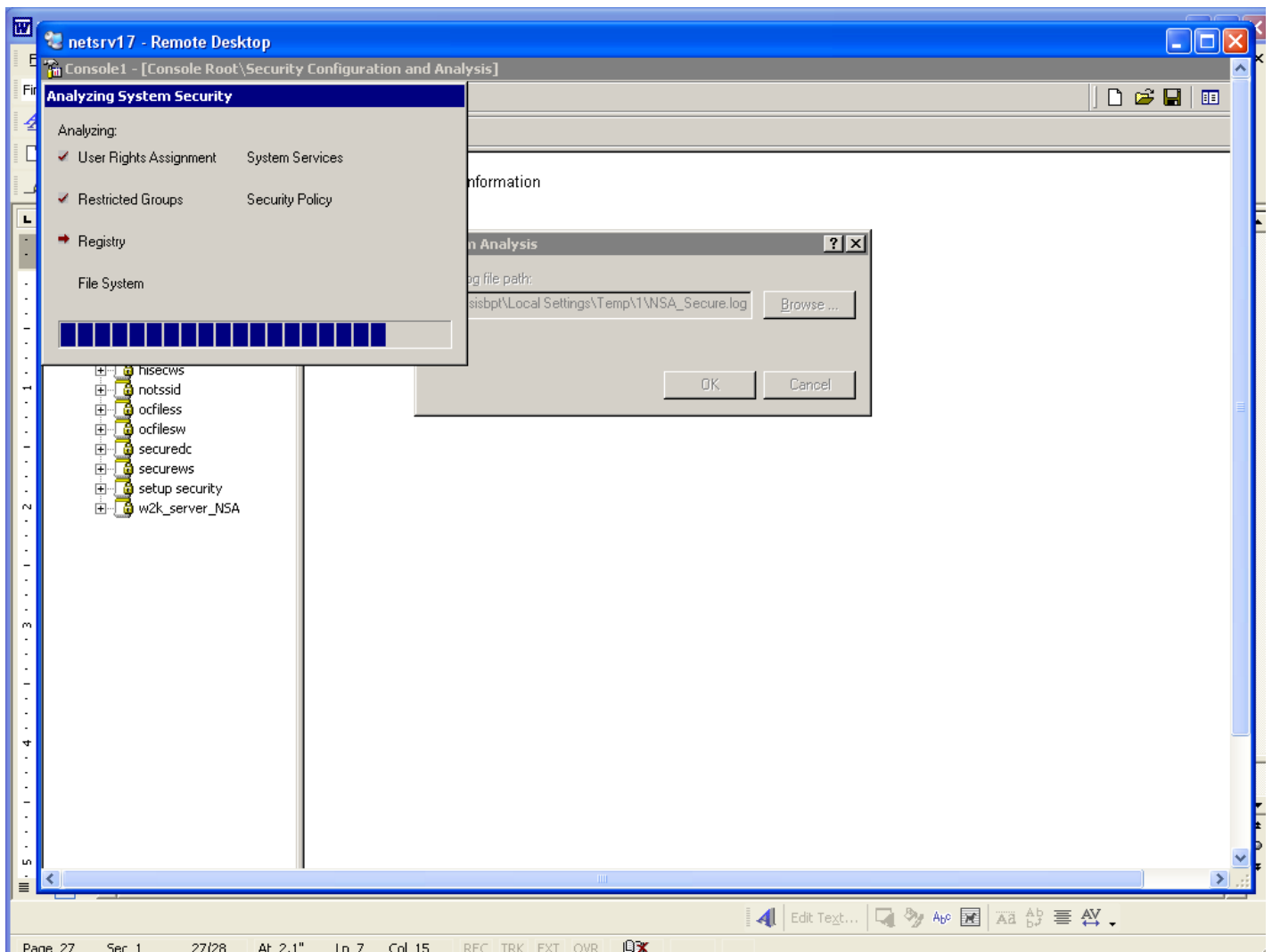
**Figure 9 – Security Setting Analysis Progress**

### 5.0 Testing Template settings

Now that I am satisfied with the template settings, I am ready to begin my actual testing of the NSA template. My intention for this test is to test at least one security setting from each grouping of security configurations. The tests will provide further proof (In addition to the Analysis previously performed) that the security settings have actually been applied.

### Test #1

♦ The first setting I will be testing is the 'Account Policy' security configuration options. My mantra on this was always, "When you hear Account Policy, Think Passwords". Account policy settings are where all password related policies are configured and stored. My Template has configured a minimum password length of **12 characters**, with a password history of **24 passwords**, previously used. For this test, I first attempted to use a 9 character password. In addition to the password being only 9 characters, I did NOT use any Non-alphanumeric characters, or Base Digit numbers and it was a password I had previously used. The second point relates to the Account policy **"Passwords must meet complexity requirments"**. This setting dictates that Passwords must meet the following requirements:

♦ Does not contain all or part of the user's account name
♦ Is at least six characters in length
♦ Contains characters from three of the following four categories:
  ♦ English upper case characters (A..Z)
  ♦ English lower case characters (a..z)
  ♦ Base 10 digits (0..9)
  ♦ Non-alphanumeric (For example, !,$#,%)

These passwords settings would be applied when a new password is created, or an existing password is changed. They would not affect existing passwords. Below is the screen shot showing my results.
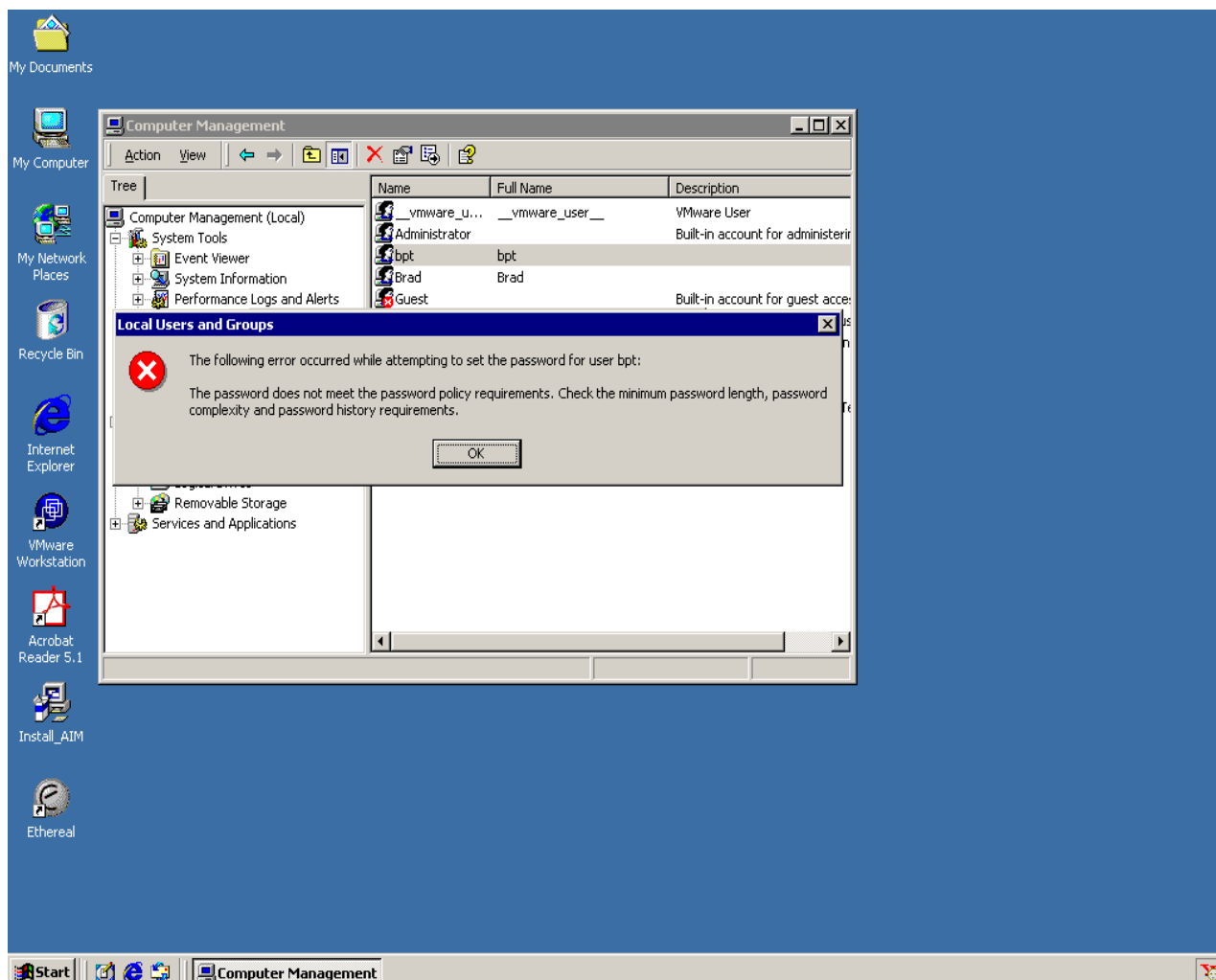
**Figure 10 – Security Setting Password Failure**

## Results from Test #1

As expected (And Hoped) the password was NOT accepted by the Operating System. In this test, I was actually testing 3 specific Account Policies. The Password length, History, and Complexity requirements. The password supplied for this test fulfilled neither of these requirements.

## Test #2

♦ Test #2 was actually relatively easy to ascertain whether or not the setting in question took place. Here I was looking for successful implementation of a logon banner. This was mentioned while describing the 'Security Options' under 'Local Policies'. The logon banner I was expecting to see was: *"Secure System! Authorized Users Only,*

*Unauthorized use of this system will be monitored and users will be punished accordingly."* With a title of "*Authorized Users Only*"

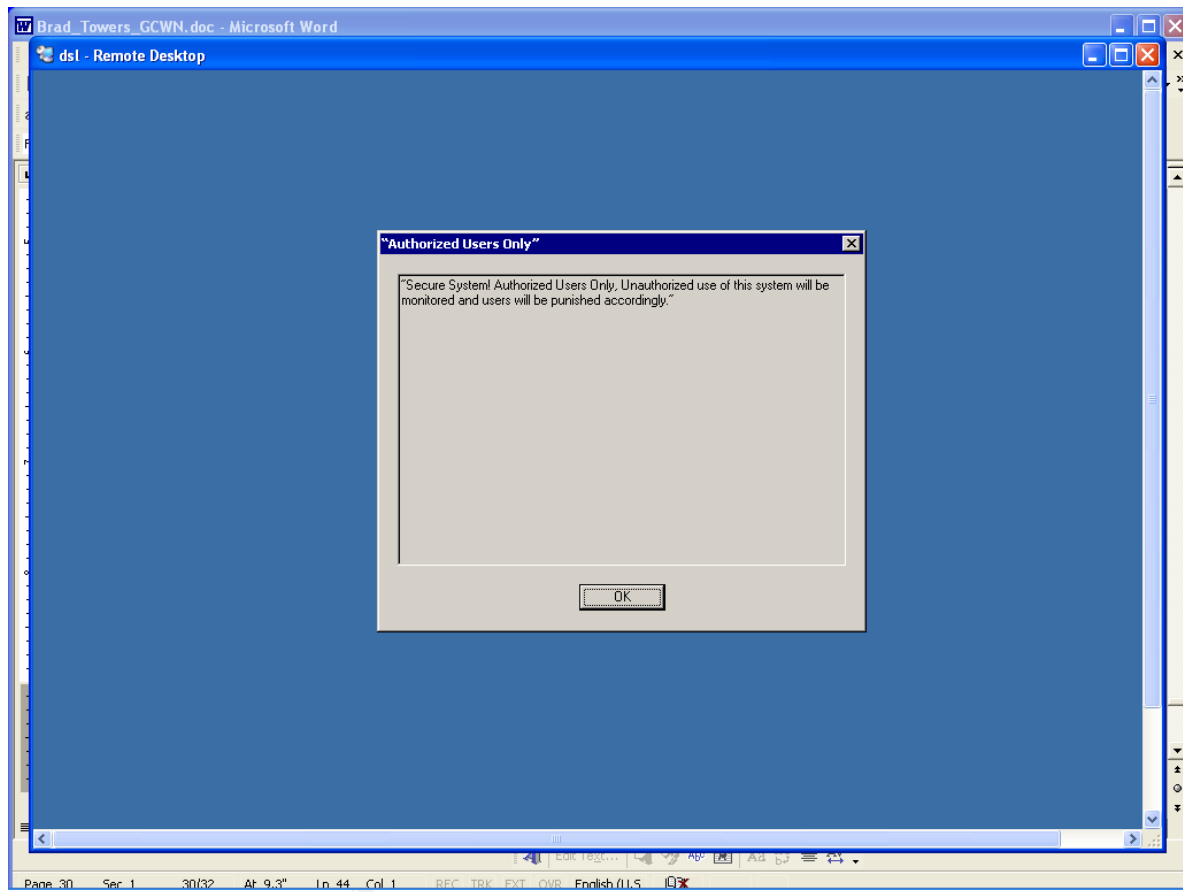♦ Figure 11 Shows the expected result.



**Figure 11 – Logon Banner**

## Results from Test #2

♦ As expected, when I hit the 'Ctrl + ALT + Del' key sequence to log on, prior to actually being logged on to the system, I had to agree to the "log on banner" by selecting 'OK'. This setting gives peace of mind in that users are aware they are being monitored. Also there is not the possibility (However remote) that unauthorized users (Hackers, Crackers, Etc…) are able to use a 'Plausible Deniability' defense if caught. They will not be able to say "I didn't know I wasn't supposed to be in there."

## Test #3

♦ For Test #3, I will be testing the Event Log settings, in particular, the Guest account having no access to the Application, Security and System Event logs. In order to perform this test, I enabled the Guest account. (Disabled by Default), and gave the

account a password that conformed to my Account Policy. Also, the in order to perform this test, I had to allow the Guest account the right to logon interactively. Best practices surely recommend against this, however since I wanted to test this particular Template configuration, I had to allow it. In addition to the "Log on Locally" right, I had to change the permissions in the "Terminal Services Configuration" administrative tool. As this server was running Terminal Services in Remote Administration mode, the only group authorized to use Terminal Services to log on, was the 'Administrators' group, and 'System' group. In order to perform this test in my environment, I had to add the 'Guests' group. I did this through the "Terminal Services Configuration" MMC, selected 'Connections'. I then opened "RDP-Tcp" and selected the 'Permissions' tab to set the appropriate rights. Again, this is surely against all best practices, yet in order to test the application of this specific setting, I needed to enable it. Once the test was complete, this setting was returned to its previous configuration.  As you can see in Figure 12, by allowing the Guest account to "Log on Locally" I brought the template database out of compliance with the Template. When I changed this setting, it only affected the local database, Until I ran the configuration option again. Once that was done, I then logged on as Guest and attempted to access the System Log in Event Viewer. As expected, the Guest was denied access to viewing events in the System Log.

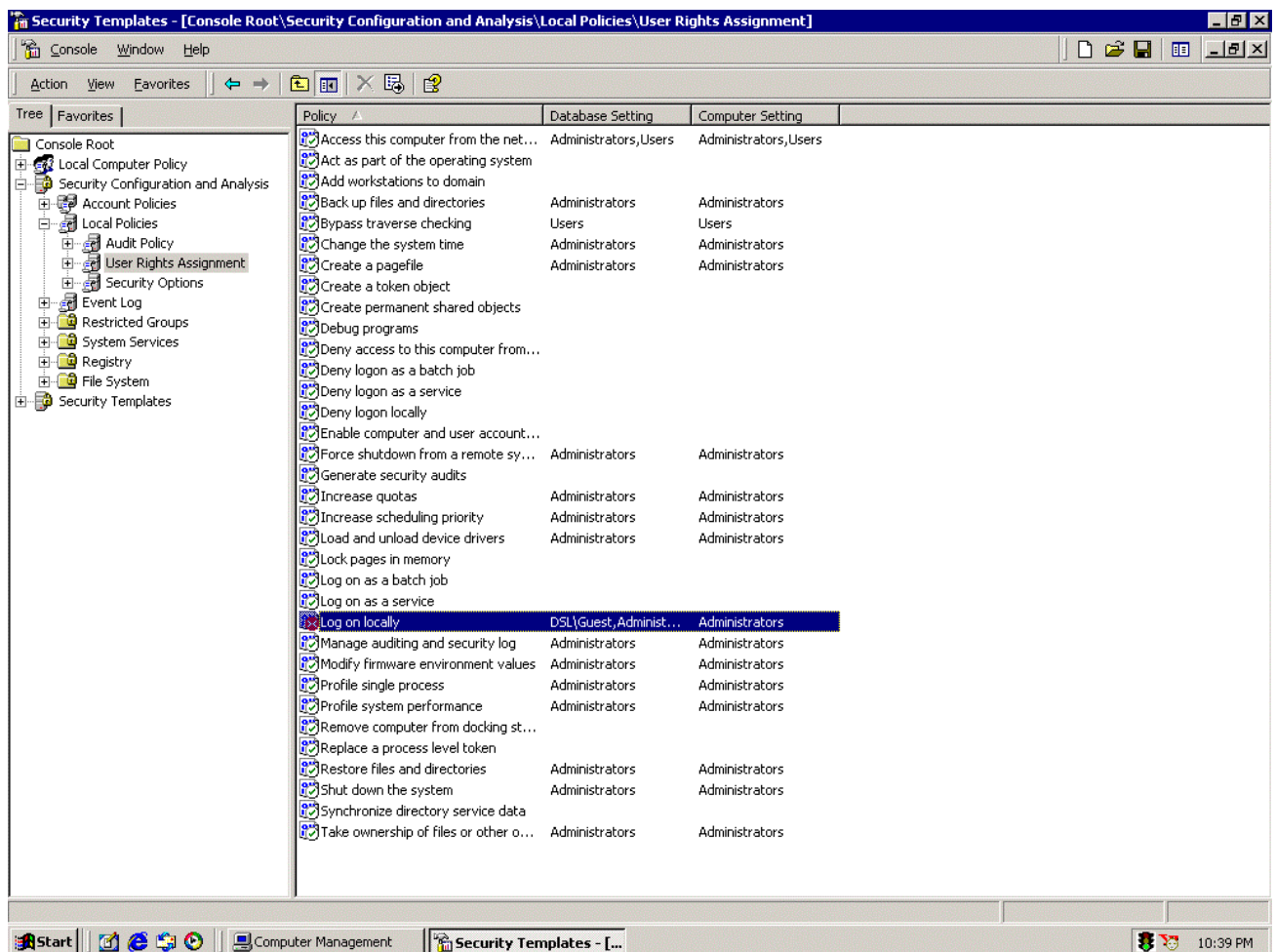 Figure 13 shows the results:

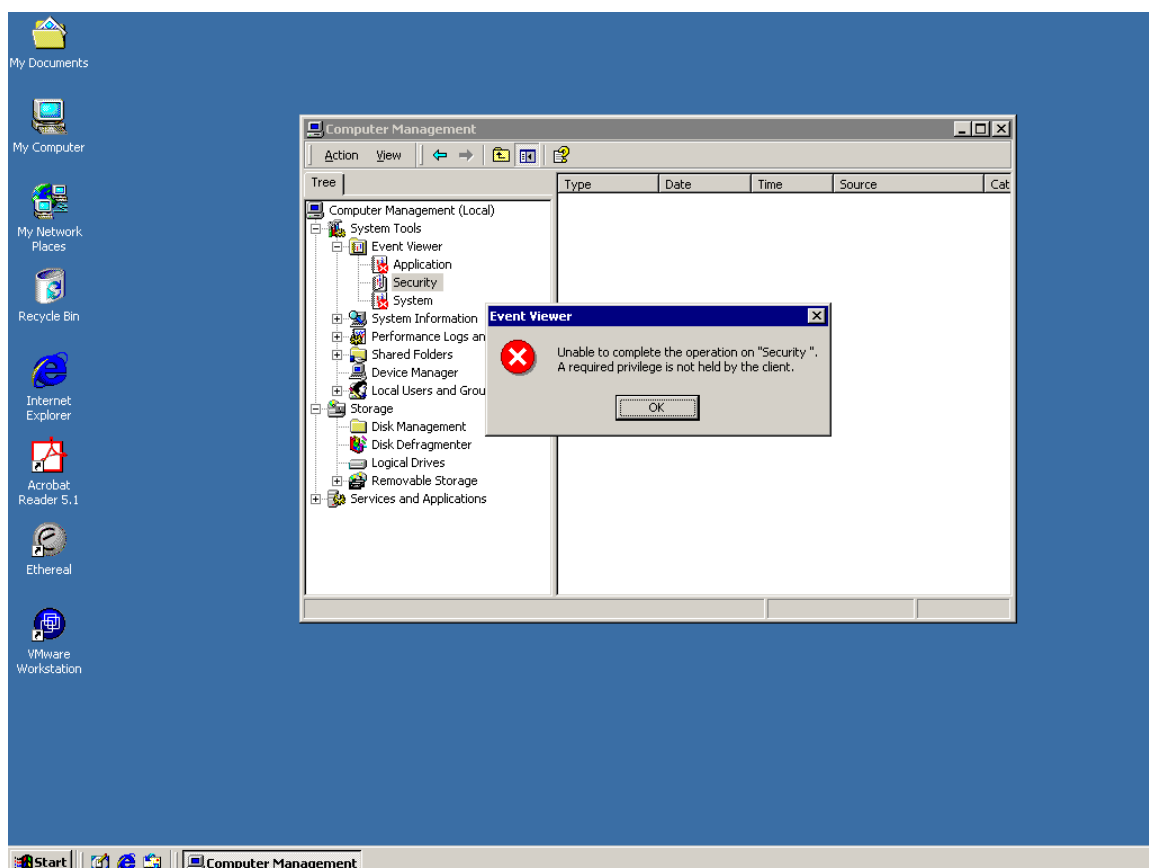**Figure 12 – Database Setting**

**Figure 13 – Access Denied to System Log**

## 6.0 System functionality after applying Template

The Template settings have been discussed, applied, and analyzed vs. the actual computer settings. Now we need to ensure that the system will still function properly in the role it needs to perform. As mentioned at the beginning of the paper, the system will be performing the role of a Web Content Filter/Monitor. The Web Content portion of the server is running SuperScout Web Filter V4.1.

### Test #1

♦ For my first test, I will need to ensure that I am able to start up the Web Content application, make a connection to the local database, and configure the rules I will use to monitor/filter web traffic. For this test I created a rule denying access to all sites categorized as "Adult / Sexually Explicit" See Figure 14
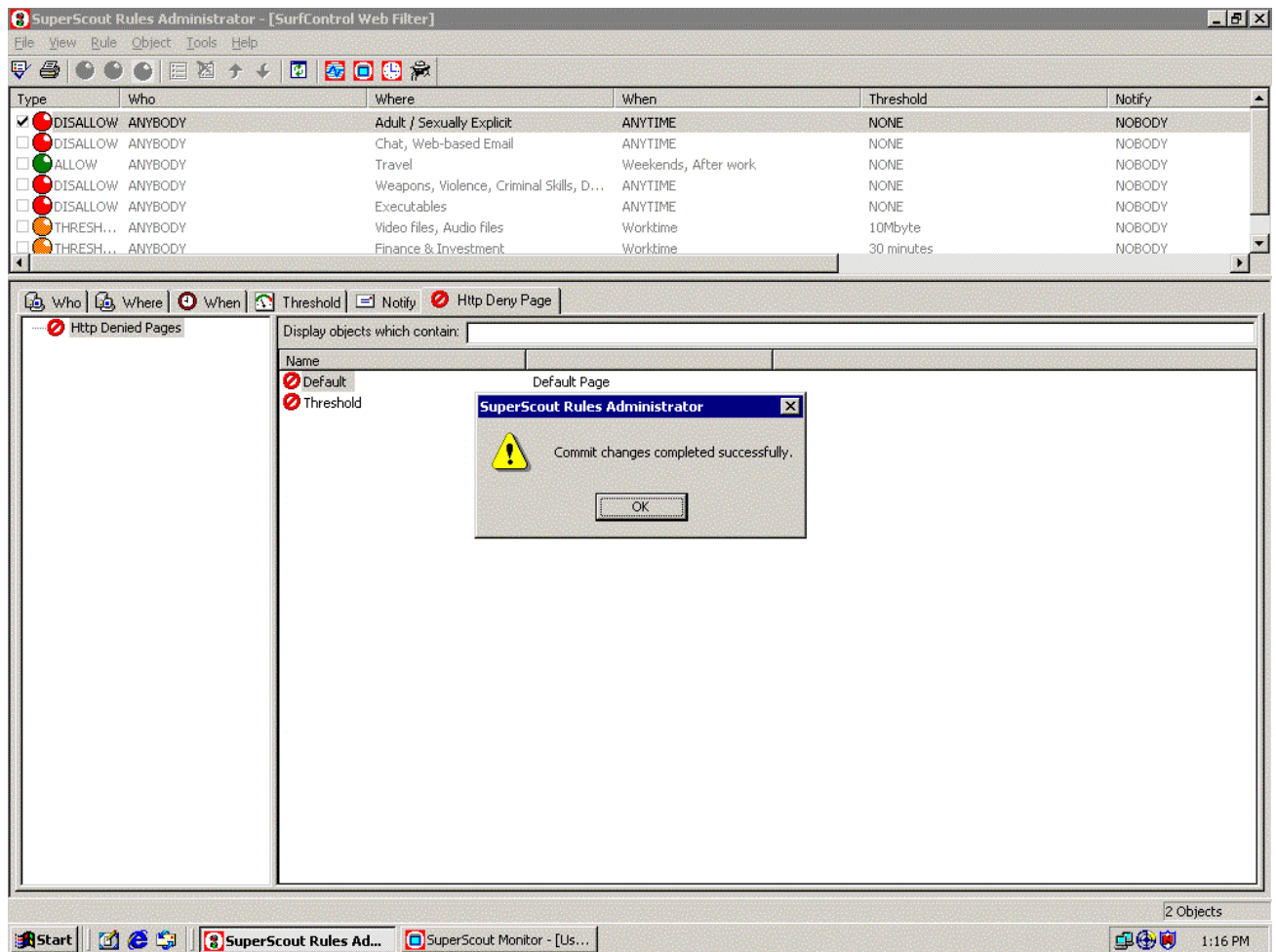
**Figure 14 – Rules Configuration**

## Results from Test #1

♦ I was successfully able to Log onto the Server, Access the Rules Administrator application, configure a rule blocking certain categories of Web Sites, and save the configuration changes to the SurfControl database.

1. Start → Programs → SurfControl Web Filter → Rules Administrator
2. Created Rule Disallowing access to sites categorized as "Adult / Sexually Explicit"
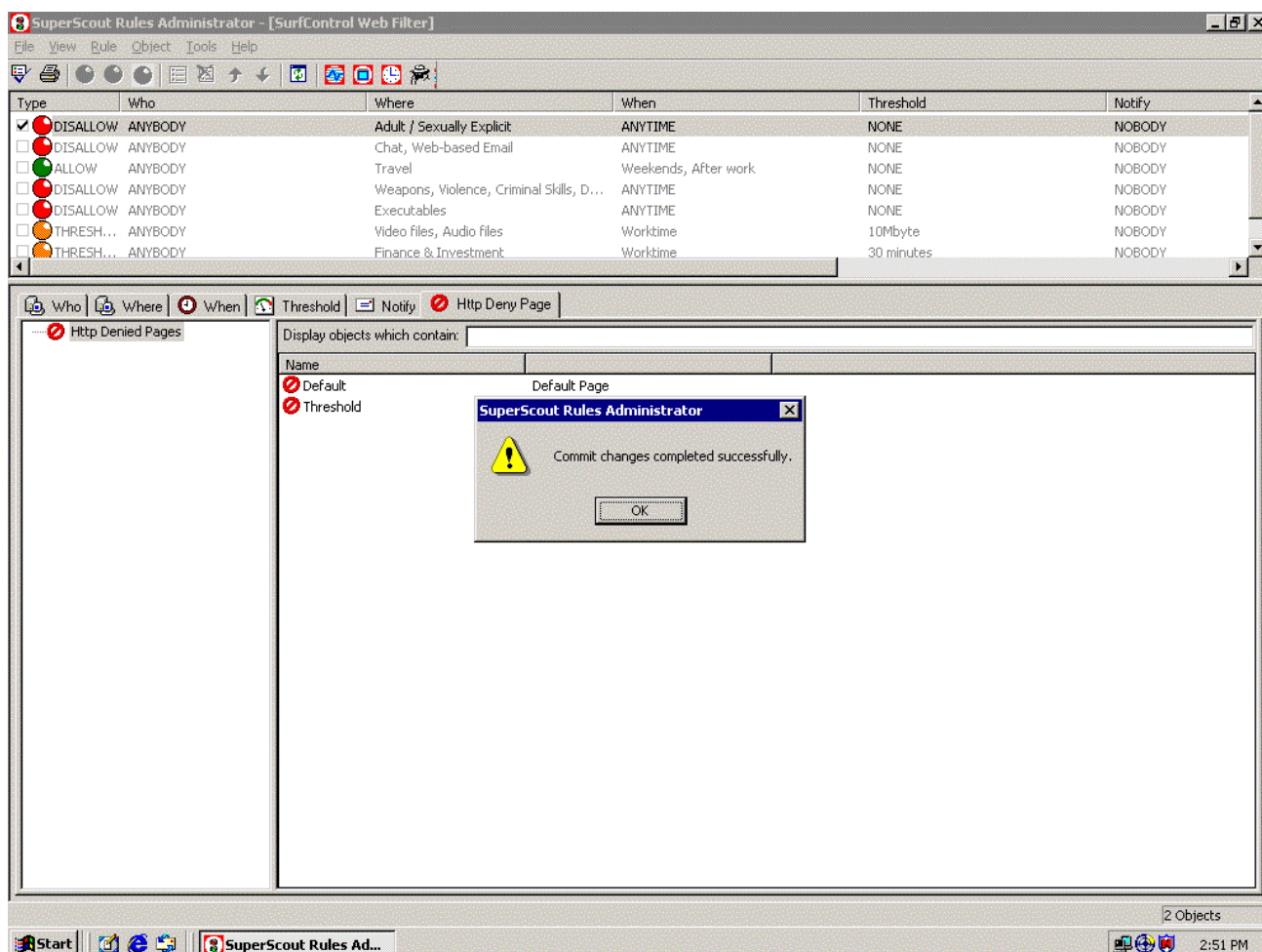3. Saved Configuration. See Figure 15

**Figure 15 –SurfControl Rules Administration**

## Test #2

♦ After configuring a rule denying access to sites categorized as Adult / Sexually explicit, I need to ensure that the rule is actually enforced. In order to do this test, I attempted to access a site that would most likely be categorized as "Adult / Sexually explicit". As expected, I was denied access to the site. See Figure 16
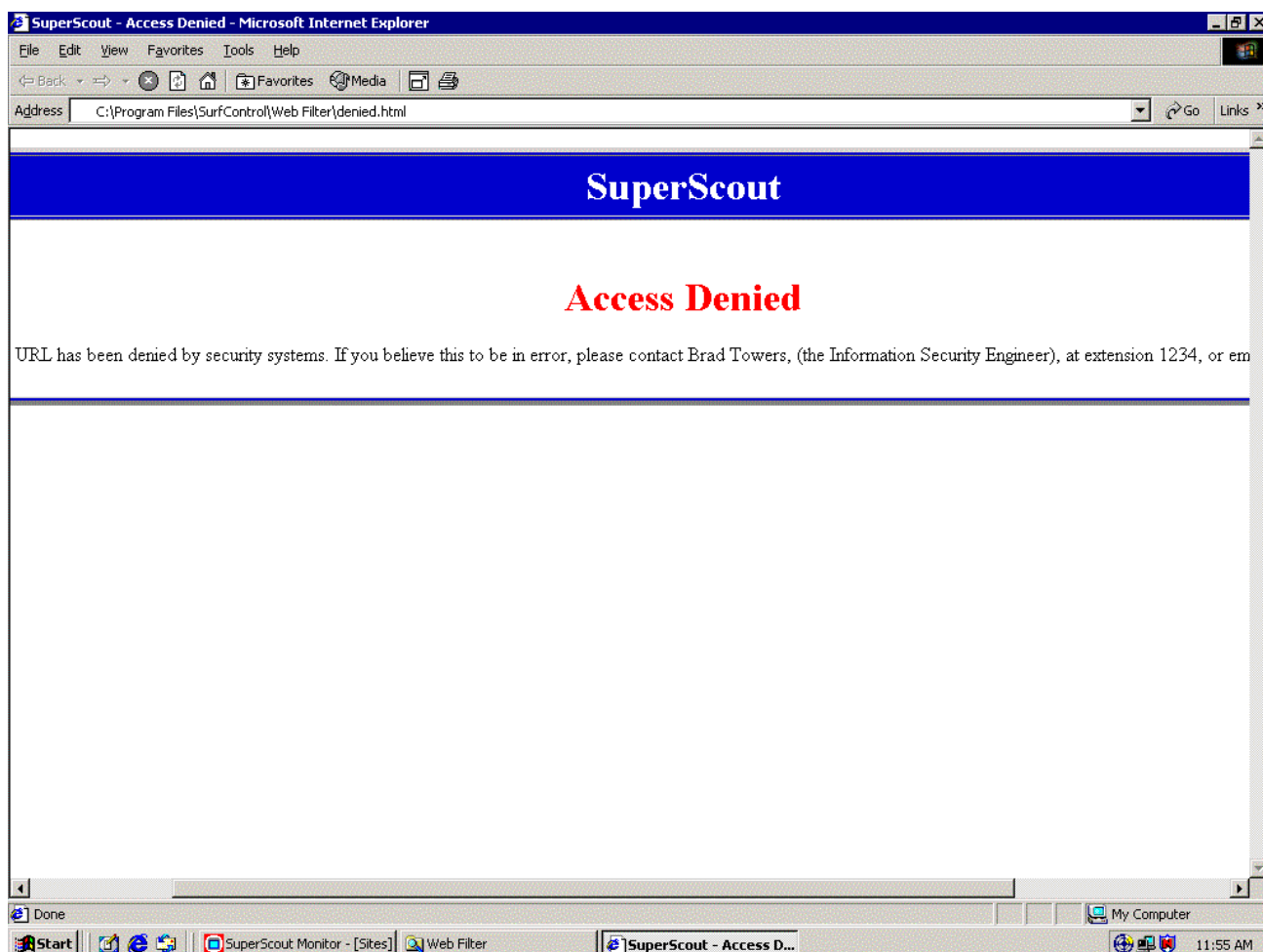
**Figure 16 –SurfControl Access Denied Page**

## Results from Test #2

♦ As expected, the Server intercepted my outbound HTTP/Get Request, and blocked access to the requested URL. The figure above shows the Web page that was returned in place of the requested URL. This showed me that the Server was intercepting outbound requests, and processing them according to the rules configured.

## Test #3

♦ For my final test, I want to ensure that I am able to access the SurfControl Monitor, and generate Reports based upon pre-defined or custom criteria.
   1. Start → Programs → SurfControl Web Filter → Monitor
   2. The Monitor application opens.
   3. Select the "Graph" button on the tool bar across the top.

4.  I entered in all data (HTTP & FTP requests) from my user account and was able to generate the following report.



**Figure 17 –SurfControl Report**

## Results from Test #2

♦ As shown in the report above, (Figure 17) I was able to log onto the SurfControl system, access the Web Monitoring application, and generate a report based upon the web traffic I generated and criteria I specified.

**System functionality Conclusions:**

♦ After applying the Template, I tested several of the security configuration settings. I then tested the functionality of the system. With this complete I am confident that the system will be able to perform in it's designated role. The system is intercepting Web traffic requests, and managing those requests based upon rules created within the Software loaded.

### 7.0 Template Evaluation

The NSA Template, " Win2k_Server.Inf" is a terrific template to use as a "baseline" for a Very Secure system. In some cases, the settings of the Template may be a bit too restrictive, in others, it could possibly be locked down even a bit further. Take for instance the "Account Policy". The Template setting remembers 24 Passwords, has a Maximum password lifetime of 90 days, and required passwords to be a minimum of 12 characters. This is ( In my opinion) a secure password policy, yet the passwords have a Minimum age of 1 day. With a password history of 24 days, I can understand the logic for this setting, yet I would recommend increasing the Minimum password age to 7 days. Another area where I would customize the Account Policy is the 'Account Lockout Policy'. This policy setting will "Unlock" an account after 15 minutes. Thus, a user (I.E. Hacker, Cracker…) could attempt to logon, after 3 tries, the account is locked out. If he/she waits 15 minutes, the account is unlocked and ready to go again. I would recommend increasing the time to the maximum or 99999 minutes. This all but ensures that a locked account must be unlocked manually by an Administrator. Again, these setting may be too restrictive for some environments, and as always you need to determine what is best for your network. No template, no matter how secure, should be taken and plugged into a network or system, without first modifying it to best fit the organization. Information Security is about risk management, and this holds true in the case of Server security as well. It is necessary to be able to achieve a balance between a secure system, and one that is able to perform the necessary functions that enable business.

### 8.0 Summary

As mentioned above, the Template supplied by the NSA serves as a terrific starting point to create and lockdown a server that requires a higher level of protection than your average file server. After configuring and testing the Template, I was satisfied that, with some modification to fit my environment, I could put a system into production with this template.

## 9.0 References

[1] Hardening Windows 2000 by Philip Cox   http://www.systemexperts.com/tutors/HardenW2K101.pdf

[2] Microsoft Baseline Security Checklist
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/w2ksvrcl.asp

[3] National Security Agency, Security Recommendation Guides
http://nsa1.www.conxion.com/index.html

[4] Microsoft Knowledge Base Article Q246261
http://support.microsoft.com/support/kb/articles/Q246/2/61.asp

[5] Microsoft Knowledge Base Article Q239869
http://support.microsoft.com/support/kb/articles/Q239/8/69.asp

[6] Microsoft TechNet online
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/server/516.asp